


# Digital information security management policy in academic libraries: A systematic review (2010–2022)

Journal of Information Science  
1–15  
© The Author(s) 2023  
Article reuse guidelines:  
sagepub.com/journals-permissions  
DOI: 10.1177/01655515231160026  
journals.sagepub.com/home/jis  


**Ghulam Farid** 

Library, Shalamar Medical & Dental College, Pakistan; Institute of Information Management, Pakistan

**Nosheen Fatima Warraich** 

Department of Information Management, University of the Punjab, Pakistan

**Sadaf Iftikhar**

Department of Information Management, University of the Punjab, Pakistan

## Abstract

Digital information security management (DISM) is considered an important tool to ensure the privacy and protection of data and resources in an electronic environment. The purpose of this research is to look into the applications of DISM policies in terms of practices and implementation in academic libraries. It also identifies the challenges faced by academic libraries in applying these DISM practices regarding policy. A systematic literature review was conducted to achieve the objectives of the study. The data were collected from well-known different databases, that is, Library Information Science and Technology Abstracts (LISTA), Library and Information Science Abstracts (LISA), IEEE Xplore, Emerald Insight, ACM Digital Library, Scopus, Sage journals, Taylor & Francis, ProQuest, Science Direct, Wiley Online Library, and Google Scholar. It followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to choose relevant articles with keyword searching. Some academic libraries have developed DISM policies on data protection, data backup, information security (IS) systems, the development of hardware and software, the training of library staff, data protection from malware and social engineering, and data security and privacy. A few libraries have developed a mechanism to protect and secure users' sensitive data from hackers, viruses, malware and social engineering. Findings indicated that both organisations and users trust libraries due to their strict privacy and data security policies. However, some academic libraries did not adopt and implement DISM policies in their organisations, even though they had written DISM policies. Libraries have been facing issues with the DISM policy on data security and privacy, data backup, IS systems, hardware and software upgrades and technical support of library staff. They also face budgetary challenges and a lack of readiness among librarians to adopt emerging tools and technology such as DISM. Library professionals faced challenges in developing and implementing the DISM policy. For data security and privacy, stakeholders, administrators and library professionals must promote the DISM policy culture in academics. This study is beneficial for library professionals, policymakers, administrators and management to make DISM policies and implement them in their organisation or libraries to secure sensitive, personal data and resources. This article is the first review of DISM policy in academic libraries of its kind and would be useful for information professionals, stakeholders and administrators.

## Keywords

Academic library security policy; adoption of DISM; barrier of DISM; data protection security; digital IS management; digital security; practice of DISM in libraries; security in libraries

---

## Corresponding author:

Ghulam Farid, Library, Shalamar Medical & Dental College, Shalimar Link Road, Mughalpur, Lahore 54000, Pakistan.  
Email: [css\\_bcs@yahoo.com](mailto:css_bcs@yahoo.com)

## Introduction

### *Background of the study*

As library resources transition from print to digital and web resources, libraries have moved from physical locations to the Internet. These modifications are primarily attributable to information technology (IT) innovations and their effects on libraries; IT expertise is the understanding of and aptitude for making use of computer hardware, software and processes to create particular computer applications [1,2]. In this age of the digital revolution, library professionals recognise the importance of web visibility in addition to their physical presence. They have been struggling to reach their users through the web to utilise their data assets and services. Libraries deliver information resources, software, services, tools and programmes to their users anytime and anywhere through the web. They also have been providing services and communicating with users via social media, digital assets and material and repositories, and play a vital role in the development of an information society.

In this scenario, libraries need to safeguard the privacy and data of their users in a digital environment. Data security has attained significance in this digital world, especially for academic libraries. Web security and the security of library materials are both significant parts of library services [3]. However, more substantial is the protection of library resources, library users and staff data. Sensitive information data frameworks (the frameworks with the most recent hardware, software, infrastructure and networking) are constantly improving methods for controlling library assets in traditional and virtual ways. In this age of innovation, the Internet is essential for data resources, data exchange and communication. Library professionals are concerned about the protection of their patterns from vulnerabilities [4].

Businesses employ technology to gather, store and share essential information in today's hyperconnected environment. The likelihood of malicious, unauthorised individuals accessing, altering, distorting or wiping data is quite high. Businesses take IS precautions to protect their sensitive data from danger in this scenario. When an organisation is the target of a data breach, there are numerous and different hazards that can damage their reputation and bottom line [5].

Digital information security management (DISM) is regarded as a crucial tool for ensuring the confidentiality and safety of data and resources in a digital world. The majority of Asian academic libraries have a low level of practise in making DISM policies and implementing them. They also have fewer DISM-related skills, awareness and knowledge [6,7]. This study intends to investigate how DISM policies are applied in terms of policies and execution in academic libraries. It also points out the difficulties academic libraries have in implementing these DISM procedures in relation to policy.

### *IS*

IS is defined as the process of securing information and data resources in order to maintain data privacy, accuracy and availability (ISO 17799, 2004) [8]. This definition of IS is adapted from that of the E-Government Act of 2002 [9] and American National Security Federal Information Security Management Act of 2002, Clause 3542, United States Code, Subchapter III as cited [10]. 'Information security' is defined as:

securing and protecting the information from unauthorised use, access, disruption, disclosure, destruction, or modification in order to provide A) integrity, which includes safeguarding against unauthorised information modification or destruction and ensuring information nonrepudiation and authenticity; B) confidentiality, which involves maintaining authorised controls on access and disclosure, including safeguards for individual privacy and proprietary information; and C) availability, which involves making information timely and trustworthy to access and use. [11]

The 2012 Information Technology Security Techniques: Information Security Management Systems Overview and Vocabulary Standard ISO/IEC 27000 (for the successful implementation of the management system) Various Techniques and Tools for Information Security Management Information Security Management Systems General Overview and Terminology addresses the IS management system. There are several elements that have an impact on IS, which enables an organisation to accomplish its business objectives [12]. One of them is a successful programme for increasing employee knowledge of, education in and training in IS, as well as bringing their duties for upholding IS as described in IS policies and regulations to their attention and motivating them to take the necessary steps [13].

The 2013 Information Technology Security Techniques Information Security Management Systems standard ISO/IEC 27001 addresses difficulties with IS awareness. Information Technology: Security Methods and Tools Requirements Section 7 of this document addresses the IS management system requirements Information [14]. They must be aware of the IS policy, their role in ensuring the efficacy of the IS management system, the advantages of enhancing the system's

functionality and the repercussions of not adhering to the IS management system's standards (ISO/IEC 27001, 2013) [14].

In order to protect their information assets, firms are forced to invest in IS [15,16]. By utilising cutting-edge IT and IS management systems, organisations are reducing the risks associated with IS [17]. IS standards play an essential role in risk mitigation since they provide advice on how such countermeasures should be created and implemented. It entails adopting the best practises outlined in international IS standards such as the ISO-27000 series [18,19]. An example of a de jure standard, or one that has been issued by governmental entities, agencies or independent standards development groups like the International Organization for Standardization (ISO), is the ISO-27000 series [20].

### *IS management system – DISM*

DISM is an important concern in academic libraries all over the world. The need to protect the digital library assets from all potential threats and ensure the confidentiality and availability of the digital information resources is a constant issue in academic libraries. The author defined the 'Digital Information Security Management System' (DISMS) as it 'provides requirements for establishing, implementing, maintaining and improving an information security management system' (p. 3) [8].

According to Disterer [21], Information Technology – Security Techniques Information Security Management Systems – Overview and Glossary Standard ISO/IEC 27000 (for the implementation and successful implementation of the management system) Methods and Tools for Information Security Management Systems Overview and Terminology in General Numerous elements affect IS, which enables an organisation to accomplish its business objectives. An efficient programme for raising awareness, educating about and training in data protection is one of them. It should encourage all employees to take the necessary steps to fulfil their obligations to ensure IS as outlined in IS policies and regulations.

IS standards are documented and incorporate best practices for IS management systems. Most organisations employ IT to streamline their daily operations. Small- and medium-sized enterprises (SMEs) use ISO 27001 standards as a sign of their dedication to optimal IS procedures [22]. To ensure that IT is employed and exploited in line with local and international rules, IS standards must be defined.

### *IS policy*

According to Soliman and Mohammadnazar [22], 'Information security policy (ISP) is recognized as the foundation of organizational information security meanwhile it communicates to the employees what they can and cannot do with the organization's assets' (p. 6813).

There are numerous definitions of an IS policy in the literature. According to Chen and Li [23], management uses an IS policy to distinguish between employee behaviours that are either authorised or restricted, as well as the penalties if the illegal behaviours occur. The goal of an IS policy, according to Disterer [21] and ISO/IEC 27002, is to provide direction and support to management in compliance with business regulations and requirements while dealing with IS. As these two definitions demonstrate, an IS policy helps considerably to improve an organisation's well-being when it comes to securing its information. However, designing and implementing an effective IS policy is at best a complex task [24].

Library professionals create a complete profile of library users on the account of an academic or digital library to identify the misuse of library and personal data. The hackers can attack in any form to access the user's data from libraries, such as via email records and web links to find records like e-books, e-journals, e-resources and other e-publications. They also highlighted the fact that before accessing e-resources from academic web links, you must pay a fee [25].

Aslam et al. [6] suggested that the policy must recommend the legal, ethical and technical landscapes for digital resources and information. Moreover, there is a need to formulate a policy to interface with digital security, system implementation, intellectual property and Internet policies for the protection of library material. The study also pointed out that data security is to be authentic, and libraries are required to have combined IS policies and technical measures, awareness construction activities and security procedures in their security programmes.

### *Why DISM policies in academic libraries*

According to the American Library Association (ALA), libraries must protect users' data and privacy from misuse. Libraries must make their library policy public and post it online:

Users have the right to be informed about what policies and procedures govern the amount and retention of personally identifiable information, why that information is necessary for the library, and what the user can do to maintain his or her privacy. [26]

The collection of library materials, services, tools and software are offered by libraries on the Internet, allowing users access to them from anywhere in the world at any time. A digital library, social media, repositories and other platforms are just a few of the ways libraries can be found online. A key role in the knowledge society has been attained by digital libraries [11].

At the appropriate time and whenever their users need it, libraries gather, process and distribute information. Digital material is available at a rapid rate, and libraries are working hard to make sure their users have access to it when they need it and where they want it thanks to network and communication technology and DISM. The libraries are creating their online presence for this reason as well, giving their consumers convenient access to the material. A library's assets must be protected, and that is the job of IS. It is now essential for libraries to seriously consider IS and take the required precautions with regard to the information resources they contain in light of the growing dangers and damages [27,28].

### *DISM security challenges*

Security is a significant issue in digital library plans. Security flaws in digital libraries, combined with attacks or different sorts of failures, can prompt confidential data to be inappropriately retrieved or damage the reliability of the data accessed. These can damagingly affect the trust of suppliers or other material suppliers, can cause discomfiture or even financial disaster to digital library administrators and can cause prompt agony if critically required data are inaccessible (p. 8) [29].

When an attempt is made and a breach is discovered, IS issues are primarily brought to light. Digital information is subject to a number of security rules, although doing so is more expensive and involved than it is with print versions. IS therefore poses a serious management concern for libraries. IS management is something we need to actively address in light of the rising number of users requesting to use the computers, networks and information and communication technologies the library offers ISM [11].

### *ISM threats in libraries*

The researchers have emphasised security hazards in technical measures for a phase where innovation and management are connected [30]. In contrast to a conventional library, a digital library faces more security threats because of the high dependency on PC innovation, e-resources, data storage, data retrieval, data communication technology, network technology, hardware, software threats and other critical control assets. When issues in data security emerge, the administration of the digital library scheme is expected to be pretentious. The researchers [31], expressing safety as a worry for a library, claimed that libraries are systems, and security is a dynamic portion of maintaining stability in the system. It aids in the adoption of policies by library professionals and other library workers to mitigate the effects of a known hazard in libraries. Consequently, library security administration requires an expert who can cope with the complications of library security and safety. Typical of a library, a security suite protects workers and their assets, such as library collections, resources, systems and computers.

This study is beneficial for library professionals, policymakers, administrators and management to make DISM policies and implement them in their organisation or libraries to secure sensitive, personal data, library data and resources. There is no study available on the systematic review of DISM policy in academic libraries in the field of library science. Merchan-Lima et al. [32] provides a strategic resource that advises higher education institutions (HEIs) on how to create an information security management framework (ISMF) and what factors to consider when putting it into practice in an era of constantly changing security concerns in academic institutes.

ISMF in academic libraries and on IS issues of IT infrastructure (hardware, software, networking, denial of service and SQL injection). However, from 2000 to 2010, this systematic review focused on data security policy, user IS, threats and social engineering in libraries [33]. Therefore, the researchers reviewed the literature of DISM policies in academic libraries from 2010 to 2022 to cover the literature gap.

### *Research objectives*

1. To elucidate the kind of digital information and security management policies in academic libraries.
2. To identify practices for adopting the DISM policy in academic libraries.
3. To explore the challenges faced by library professionals in designing and implementing DISM policies in their libraries.

## Literature review

In order to determine the level of awareness of those working in academic libraries regarding the management of digital IS and the policies. The study stressed the significance of watchful library staff and users as a major concern for the safety of the general populace. The study conducted with the intention of evaluating the electronic security measures in place at academic libraries at three universities in southwest Nigeria. A total of 109 heads of technological services departments, university librarians, and other staff made up the survey sample, along with 81 respondents from academic libraries at Babcock University, the University of Lagos and Covenant University. University libraries should improve their security services in order to maintain their information systems, according to the study's findings, which showed that they had security issues. The investigation's findings also revealed that the three aforementioned colleges have electronic systems installed in their libraries [34].

The King Saud University Library seeks to highlight the issue of security as well as the security of libraries, its technologies, staff and patrons. The administrative and technical employees of the library served as the study sample, which was collected through interviews. The study's findings showed that information systems and libraries are vulnerable to security and safety risks, and that the solutions offered for keeping libraries secure can be achieved by utilising modern technologies and establishing reasonable standards. The survey also indicated that library collections had poor follow-up, placing them at risk for security breaches. In addition, there was no expert team to manage the automated library systems, which caused some issues with the policies already in place [35].

An additional layer to the two sides of this matter, however, is that there is no official policy or code that can direct educational libraries' efforts to confirm confidentiality, irrespective of technical developments [36]. Moreover, Zimmer [37] found that while these issues are discussed in the literature, they are addressed in only a superficial manner, with no actual roadmap or recognised set of best practises for library professionals. Thus, in spite of acknowledging a person's entitlement to security as both a lawful and essential human right, the way ahead for libraries is not always clear. Ismail and Zainab [30] recommend a library information system security evaluation model, which encompasses five domains: DISM security policy, technological measure, approaches and awareness of DISM, procedures and control and administrative tools. Hampwaye [38] used a survey design, a questionnaire and an interview to collect data on DISM issues in Nigerian libraries.

The survey conducted on library professionals in China. According to the study, there is no policy for database disappointment, data backup, poor technical measures, no data protection policy, technical measures, data storage, trained staff and users, an operating and control system, a server and a password. Libraries must implement appropriate organisational and technical scales, as well as establish digital environment policies [28].

According to Aslam et al. [6], who conducted a study on DISM in academic libraries in Pakistan, the IT infrastructure in academic libraries is out of date, and the libraries also need to make policies on technical and organisational systems, the Internet and data that they must implement in their libraries to protect sensitive data in this digital age. Libraries have digital collections and then print collections in this digital age, and they also focus on security awareness programmes for library professionals and users to protect the information. A number of libraries have DISM policies on information systems, user registration and passwords, data security, data sharing, storing, data backup and software to track stolen library material and personal belongings, but unfortunately nearly half of them do not follow the policies, resulting in mutilation of library resources, theft, misuse of the computer system and misuse of users' accounts [27,7,25,39]. Kuzma [40] noted that a significant issue among developing countries' libraries is budget allocation for technological issues.

The author demonstrated a variety of approaches to research in India. This study provided a quantitative and qualitative method for investigating the application position of DISM activities over participant feelings. The investigation additionally pointed out that, for data security to be successful, libraries need to consolidate specialised measures just as they do data security approaches, security techniques and mindfulness creation exercises in their security programmes [7].

The theoretical study to identify the status of risks and threats in IS and policy. The researchers dealt with the theoretical, material and legislative aspects of IS at national and international levels. The study concluded that there are risks threatening IS in the digital environment and that legislation in regard to this aspect is weak at both national and international levels [41].

## Method

This review was performed following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [42]. The systematic review approach can also be a part of qualitative research that emphasises comprehensive and structured methods to review literature and systematic analysis of published research [43].

### Information sources

The search was done from well-known different databases, that is, Library Information Science and Technology Abstracts (LISTA) (<https://www.ebsco.com/products/research-databases/library-information-science-and-technology-abstracts>), Library and Information Science Abstracts (LISA) (<https://about.proquest.com/en/products-services/lisa-set-c/>), IEEE Xplore (<https://ieeexplore.ieee.org/Xplore/home.jsp>), Emerald Insight (<https://www.emerald.com/insight/>), ACM Digital Library (<http://dl.acm.org>), Scopus (<https://www.scopus.com/home.uri>), Sage journals (<https://journals.sagepub.com/>), Taylor & Francis (<https://www.tandfonline.com/>), ProQuest (<https://www.proquest.com/>), Science Direct (<https://www.sciencedirect.com/>), Wiley Online Library (<https://onlinelibrary.wiley.com/>) and Google Scholar (<https://scholar.google.com/>) (search engine) in January 2020 and updated in April 2022.

### Search string

To meet the objectives of the study, systematically reviewing the related literature with the help of different sets of keywords was applied, that is:

- ‘digital information security policy’
- ‘information security management policy’
- ‘InfoSec policy’
- ‘digital security policy’
- ‘Information security management in libraries’
- ‘academic library security policy’
- ‘security policy in libraries’
- ‘data protection policy’
- ‘Information security infrastructure policy’
- ‘library security policy’
- ‘data backup security policy’
- (Survey\* OR Questionnaire\* OR adopt\* OR evaluate\* OR test\* OR interviews\* empirical study).

The studies on DISM policies in academic libraries were eligible and included for this review. The publication year restriction was in effect from 2010 to 2022. Nevertheless, only English language studies were selected, and other languages were excluded.

### Inclusion criteria

- There were limited studies on DISM in library perspectives.
- Studies which covered the area of DISM Policy in academic libraries.
- Studies which used the tool or practice of DISM.
- English language studies were included.
- Studies published from 2010 to onwards.

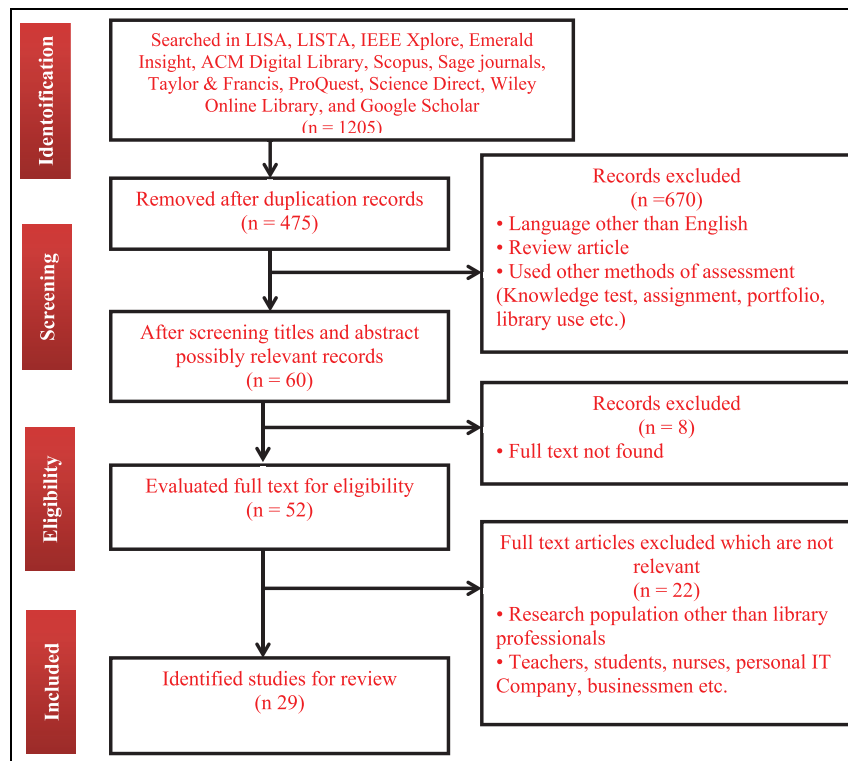
Consequently, journals’ articles, conference papers, meeting papers, dissertations and so on were included.

### Exclusion criteria

Only academic library-related studies were selected for this SR.

- Studies that do not have an abstract.
- The studies, rather than English, are not included.
- The studies with fewer than four pages were excluded.
- The book chapters were not included.

Studies discussing another type of library were not included. Most of the studies on DISM policy available in IT, Business, Health, Education and Cloud Computing (Ivanov 2011) were excluded.



**Figure 1.** PRISMA chart on DISM policy in academic libraries.

### Study selection and data extraction

A flow chart in Figure 1 (PRISMA diagram) displays the scanning procedure and reasons for exclusion and selection of qualified studies. There were two phases of data scanning, such as title, abstract and full-text papers. As evaluated in the selection criteria, 25 studies were selected for inclusion. A material extraction structure was carried out for each qualified study to gather data on the subject of the DISM policy. A data extraction table was prepared for each eligible study to collect information on the title, name of the author(s), publication year, country, population, participants, outcomes, challenges and conclusions.

## Results and discussion

### Overview of the studies

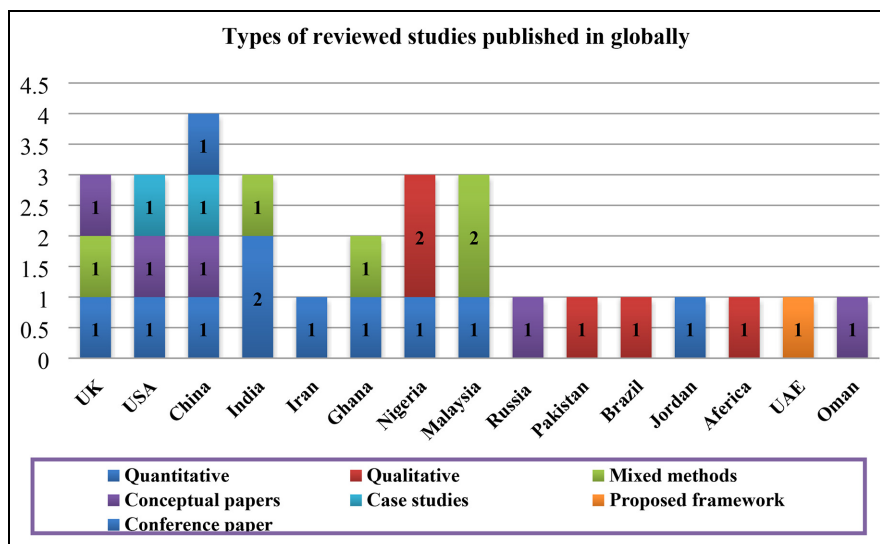
A search in nine different databases and search engines was conducted, yielding 1205 studies on DISM from well-known databases such as LISTA, LISA, IEEE Xplore, Emerald Insight, ACM Digital Library, Scopus, Sage journals, Taylor & Francis, ProQuest, Science Direct, Wiley Online Library and Google Scholar.

After the removal of duplicates, the number of the remaining studies stood at 475, after initial scanning and exclusion of records on the basis of various reasons, 670 studies were selected. Criteria were further narrowed down, and only 52 studies were found relevant to the overall DISM. However, 29 studies were ultimately chosen to meet the research objectives and inclusion criteria based on the DISM policy in academic libraries. The selected studies were from 2010 to December 2022, and most of the studies were published in library and information science, information communication and IT journals, with some in business.

The studies were conducted in the United States, Malaysia, India and Nigeria, whereas two were conducted in China, one each in Ghana, Brazil, Iran, Oman, Pakistan and the United Arab Emirates (UAE).

### Studies methods

**Quantitative method.** In this review (Figure 2), 10 studies on the quantitative method with survey design and data were collected through a questionnaire and most of the participants were academic library professionals, library heads and managers who worked with DISM and computer systems in academic libraries.



**Figure 2.** Types of reviewed studies published in globally and methodological identified studies from 2010 to 2022.

*Qualitative method.* Figure 2 shows that five studies were reviewed qualitatively with observation and semi-structured interviews. Participants in the studies were academic libraries, university libraries, library professionals and library users who deal with DISM.

*Mixed methods.* Figure 2 shows that five studies reviewed mixed methods. Most of the reviewed study participants were academic libraries, university libraries and library professionals who dealt with DISM systems in their organisations.

*Case studies and conceptual papers.* Figure 2 shows that, in addition to two case studies, five were conceptual papers, one study included conference papers and one study proposed a framework for academic and digital libraries.

### Core DISM themes identified from studies

Some libraries have DISM policies [7,44–46], and as pointed out by Vyas and Pathak [39], some libraries have DISM policies on information systems, user registration and passwords, data security, data sharing, storing, data backup and software that steals library material and personal belongings [12,41,47,30]. But unfortunately, 40% of libraries do not follow the policies. Agboola and Aduku [25] pointed out that 90% of users agreed to not allow electronic external drives. 70% of users used another account to circulate library materials, while 30% changed the passwords of their friends; so, the mutilation of library resources, theft, computer systems, misuse of user accounts and so on.

In a similar vein, Kuzma [40] stated that libraries in developing countries faced budget issues for DISM as well as technological issues. Each individual library has a policy and law to protect data, including consumer data protection and personal information, as well as the personal data of users’ technical and strong data. However, Maidabino and Ngah [47] pointed out that the plan of the DISM security policy is assessed on a regular basis in the libraries and that the DISM policy is implemented for organisational and technical measures [6,30]. In a similar vein, Ali and Soomro [48] determined that DISM policies are compulsory for libraries in this digital era. As a result of this disparity, according to Abioye and Adeowu [49] and Zaveri [50], there were no DISM policies in libraries on data security, library data planning, users’ information, technical measures and Internet usage in this technologically changed era [24,51].

Gressel [52] pointed out that libraries must develop and implement policies for the protection of data about staff and users. Hess et al. [53] reported that there was no proper policy, legally and professionally developed, for ensuring the privacy of library staff and users, confidentiality and proper guidelines in US libraries. According to Sutlieff and Chelin [54], San Nicolas-Rocca and Burkhard [55] library professionals and library users have limited knowledge on DISM policies, and some libraries have broken users’ trust. The libraries must train their staff and users for the protection of data and the privacy of sensitive information [56]. Similar to Abioye and Adeowu [49] and Al-Suqri and Akomolafe-Fatuyi [57], there was no proper training or policy for library professionals for the benefit of libraries.



**Table 1.** Core themes of adoption and implementation of DISM policies in academic libraries.

Themes	Subthemes
Adoption of DISM policy	<ul style="list-style-type: none"> <li>Libraries have written DISM policies.</li> <li>Policies on information systems, user registration and password.</li> <li>Policies on data security and data sharing.</li> <li>Policies on data storing, and data backup and software.</li> <li>Policies on stolen library material and personal belonging.</li> </ul>
Awareness and knowledge	<ul style="list-style-type: none"> <li>Libraries must have awareness of DISM policies.</li> <li>Libraries must have awareness and knowledge about data protection, backup of the data, storage of data and users privacy.</li> <li>Libraries have limited knowledge, and awareness regarding DISM policies on data security, security system implementation.</li> <li>Libraries have limited awareness and knowledge about data protection, backup the data, software and social engineering.</li> </ul>
Training	<ul style="list-style-type: none"> <li>Libraries do not have training regarding data protection, user's privacy, library systems, hardware and software.</li> <li>Libraries have limited policies of training on user's data, libraries data, users, trust and others.</li> <li>Libraries have limited policies train the library staff and users regarding DISM.</li> </ul>
Data protection and user privacy policy	<ul style="list-style-type: none"> <li>Some libraries in developing countries have DISM policies on data protection, user information and library material.</li> <li>Users have below-average knowledge on DISM, data protection, sensitive users information, protect and personal information.</li> <li>European libraries do not have a policy on data protection and sensitive information, and as analogous.</li> <li>Libraries failed to protect the user data and privacy. Libraries have poor planning on the protection of library material, sensitive data, user's information and trust.</li> </ul>
Backup of the data	<ul style="list-style-type: none"> <li>Some libraries have a data backup policy.</li> <li>Some libraries took 79% backup of the data and 63% libraries took backup on daily basis.</li> <li>Poor level of data backup policies in libraries.</li> <li>Libraries have no policies on data backup.</li> </ul>
Malware and social engineering policy	<ul style="list-style-type: none"> <li>Some librarians faced problems of computer hacking, virus attack, worm and Trojan in the libraries and organisation.</li> <li>Some libraries have a policy of not entering certain groups of websites. As per policy, there is no permission to access the social networks at the workplace.</li> <li>Poor planning for social engineering and sometimes systems were not protected from malware or Trojan in libraries.</li> <li>Problems may be faced without DISM policy in libraries like data misuse by hackers, destructive attack, invasion, tampering, malicious infiltration, malicious code and vulnerability detection to software or hardware and electronic resources, data and files.</li> <li>Libraries implement the IT framework and service to protect the data and other social engineering issues and ensure the DISM security policy in libraries.</li> </ul>

DISM: digital information security management; IT: information technology.

Some libraries have data security and protection policies in the digital era, according to Han [28], Wang [44], He et al. [58] and Amini et al. [59] to protect the library's materials and users' information as disparity [7]. Libraries do not implement policies to safeguard library materials [53,60].

As a parallel, the users have below-average knowledge on DISM, data protection, sensitive user information and personal information [55]. Similarly, in this technological era, some libraries have failed to implement digital data and user protection policies [54]. According to Al-Suqri and Akomolafe-Fatuyi [57], some European libraries lack a data protection and sensitive information policy and, as a result, have significant security flaws in their web applications. Sutliff and Chelin [54] found that libraries failed to protect user data and privacy. Libraries have poor planning for the protection of library material, sensitive data, user information and trust.

Some libraries have a data backup policy; Singh and Margam [7], Yamson and Cobblah [45], Zaveri [50] and Amini et al. [59] concluded that some libraries backup 79% of their data, with 63% performing daily backups. However, Ismail and Zainab [30] pointed out the poor level of data backup policies in libraries. According to Aslam et al., there was no policy for data backup in libraries. Fakeh et al. [61] believe that mostly librarians faced problems of computer hacking, virus attacks, worms and Trojans in their libraries and organisations. Some libraries have a policy of not entering certain groups of websites. As per policy, there is no permission to access the social networks at the workplace

**Table 2.** Core themes of challenges faced regarding DISM policies in academic libraries.

Themes	Subthemes
Issues of adoption of DISM policy	<ul style="list-style-type: none"> <li>• European countries, the libraries face issues regarding DISM policy, standards and law.</li> <li>• Academic libraries does not have technical and organisational DISM written policy and do not implement it in the libraries for protection of material and user information and data.</li> <li>• There is no strict access control policy for failure and upgradation of the systems and IT infrastructure. Some problems may be faced without DISM policy like data misuse by hackers, invasion, tampering, malicious infiltration, malicious code and vulnerability detection to software or hardware and electronic resources, data and files.</li> <li>• Libraries also faced problems because they do not have copyright policy for digital content in modern areas.</li> </ul>
Lack of awareness and knowledge	<ul style="list-style-type: none"> <li>• Some libraries and library professionals faced problems due to lack of awareness and lack of information about DISM.</li> <li>• Some problems accrued due to poor attitude of library staff towards the user regarding awareness and knowledge of DISM policy.</li> </ul>
Data protection and user security or privacy issue	<ul style="list-style-type: none"> <li>• Most of the libraries in developing countries failed to adopt new technology in the modern era.</li> <li>• There is no users' privacy policy regarding data protection, shared information, social media, resource sharing and web technologies in this modern era.</li> <li>• Libraries faced privacy and security problems regarding data protection personal information and sensitive information.</li> <li>• Libraries failed to protect digital data as they don't have a written DISM privacy policy for the security and privacy of librarians.</li> </ul>
Backup of the data	<ul style="list-style-type: none"> <li>• Most of the UK libraries failed to secure library data and user information.</li> <li>• Most of the libraries fail to take proper backup of the data on regular basis.</li> <li>• Libraries failed to have proper backup data.</li> </ul>
Technical issues	<ul style="list-style-type: none"> <li>• DISM policy as they do not adopt technical measures to secure the hardware, software, tools and networking.</li> <li>• Libraries also faced technical tools, hardware development, work stations, internet, data and network security issues.</li> <li>• Challenges in libraries such as technical measures, data storage, operating and control system, server and password.</li> <li>• Libraries have no policy for hardware and software failure and save data, subsequently failed to protect their network and IPs.</li> </ul>
Malware and social engineering policy	<ul style="list-style-type: none"> <li>• Libraries faced problems because they do not adopt IT frameworks and services.</li> <li>• Libraries are facing difficulties due to the absence of DISM policy such as data misuse by hackers' destructive attack, invasion, tampering, malicious infiltration, malicious code and vulnerability detection on software or hardware and electronic resources, data and files.</li> <li>• Libraries failed to protect the data and material because they faced issues regarding malware, vulnerable and social engineering.</li> </ul>
Budgeting issue	<ul style="list-style-type: none"> <li>• Libraries faced problems regarding social engineering and copyright policy.</li> <li>• Libraries faced problems because of a lack of budget and for installation of RFID, CCTV cameras and digital systems.</li> </ul>

DISM: digital information security management; IT: information technology; CCTV: closed-circuit television; RFID: radio-frequency identification.

[12,24,27,41,51,60]. Ismail and Zainab [30] pointed out that there was poor planning for social engineering and that sometimes systems were not protected from malware or Trojans in libraries. Some problems may be faced without a DISM policy in libraries, like data misuse by hackers, destructive attacks, invasions, tampering, malicious infiltration, malicious code and vulnerability detection to software or hardware and electronic resources, data and files [28]. Ali and Soomro [48] are of the view that libraries implement the IT framework and service to protect the data and other social engineering issues and ensure the DISM security policy in libraries.

### *Core themes of challenges faced by libraries regarding DISM policy*

In developed European countries, the libraries face issues regarding DISM policy, standards and law [24,40,41,57]. Academic libraries, however, lack a written technical and organisational DISM policy and do not implement it in their libraries to protect material and user information and data [30,52,53,55,62].

Libraries do not have a physical or environmental security policy in this digital world [48]. Abioye and Adeowu [49] describe that libraries do not have a proper plan for DISM policy. There is no strict access control policy for failures and

upgrades of the systems and IT infrastructure. Some problems may be faced without the DISM policy, like data misuse by hackers, invasion, tampering, malicious infiltration, malicious code and vulnerability detection to software or hardware and electronic resources, data and files [28]. One interesting challenge was found by Hess et al. [53], libraries also faced problems because they did not have copyright policies for digital content in modern areas.

Ali [48] and Sutliff and Chelin [54] pointed out that some libraries and library professionals faced problems due to a lack of awareness and information about DISM [12,24,41,51,55,59,63]. Some problems accrued due to the poor attitude of library staff towards the user regarding awareness and knowledge of the DISM policy [49]. Kuzma [40] identified that most of the libraries in developing countries failed to adopt new technology in the modern era.

Gressel [52] stated that there is no user privacy policy regarding data protection, shared information, social media, resource sharing and web technologies in this modern era. Similarly, Han et al. [28], Wang [44], Hess et al. [53] and Wu et al. [64] identified that libraries faced privacy and security problems regarding data protection of personal and sensitive information [12,41]. Similarly, Zaveri [50] identified that libraries failed to protect digital data as they do not have a written DISM privacy policy for the security and privacy of librarians [25]. Kuzma [40] found that most of the UK libraries failed to secure library data and user information. Universitárias [62] and Aslam et al. [6] believe that most libraries fail to take proper backups of their data on a regular basis [30]. Likewise, Zaveri [50] and Al-Suqri and Akomolafe-Fatuyi [57] think that libraries failed to have proper backup data.

The review of the literature identified that libraries may be facing challenges without the DISM policy as they do not adopt technical measures to secure the hardware, software, tools and networking [28,30,63]. The researchers [53] are of the view that libraries also faced issues with technical tools, hardware development, workstations, the Internet, data and network security. The author identified challenges in libraries such as technical measures, data storage, operating and control systems, servers and passwords [28]. Zaveri [50] identified that libraries have no policy for hardware and software failure and saving data, subsequently failing to protect their network and IPs. The researcher [48] focused on the fact that libraries faced problems because they did not adopt IT frameworks and services.

Al-Suqri and Akomolafe-Fatuyi [57] identified that libraries faced challenges such as unauthorised attacks and that technical measures were crucial in digital libraries. Kuzma [40] stated that some libraries in developing countries faced problems regarding technical issues, network problems and library system issues. According to Vyas and Pathak [39] and San Nicolas-Rocca and Burkhard [55], libraries failed to install closed-circuit television (CCTV) cameras and radio-frequency identification (RFID) systems. Libraries do not adopt technical measures to secure library material and user data. Agboola and Aduku [25] also pointed out that the use of external drives was the main issue for data security and sharing the users' passwords.

The study identified that libraries faced problems regarding social engineering and copyright policy [53]. The study [28] focused on the fact that libraries are facing difficulties due to the absence of DISM policy, such as data misuse by hackers, destructive attacks, invasion, tampering, malicious infiltration, malicious code and vulnerability detection on software or hardware and electronic resources, data and files. Universitárias [62] identified that libraries failed to protect the data and material because they faced issues regarding malware, vulnerability and social engineering. Some studies mentioned that libraries faced problems because of a lack of budget and for the installation of RFID, CCTV cameras and digital systems [39,55,59].

## Conclusion

In this digital era, some academic libraries around the globe have DISM policies on data protection, user security, obsolescence of software and hardware, data storage, data sharing, data security, a secure network, backup of data and failure of systems. Some libraries do not have DISM policies on the topics mentioned above.

Librarians and libraries are facing issues regarding the DISM policy on data security and privacy, data backup and protection from malware, viruses and social engineering, IS systems, hardware and software upgrades and technical support for library staff. Libraries also faced budgeting issues for DISM due to a lack of funds, resulting in librarians and libraries not being up to date with the latest library tools and experiencing DISM problems in developing countries. The libraries in the United Kingdom, the United States, China and UAE have policies, practises, guidelines and rules on DISM that they implement in their libraries. Unfortunately, in some countries, that is, Pakistan, India, Nigeria, Ghana and Oman, some libraries fail to make, implement and adopt policies on data protection, user security and safety, data backup, hacker attacks, IT framework and library staff training for DISM.

Academic libraries must develop written policies with ethical and legal aspects and should implement them to secure library and user data and resources. Libraries should develop policies on the upgrade of information systems, hardware and software development, and also secure the data storage, data sharing, data security, secure network, backup of data and failure of systems. Academic libraries should protect the data and resources from destructive attack, invasion,

tampering, malicious infiltration, malicious code and misuse of data by hackers' as well as from vulnerability detection in software or hardware and electronic resources, data and files. The academic libraries must adopt a proper, strong IT framework to secure the data, systems and resources from malware, viruses, social engineering and attacks from hackers. Libraries also focus on staff training on DISM on a regular basis. Libraries must have policies to maintain users' trust in data security and privacy. Libraries must keep up with technological advancements. Libraries should adopt the latest tools as per market need.

### *Recommendations*

- Libraries should adopt and implement DISM policies in their libraries. Policies must address legal, technical and ethical concerns and must be posted on the notice board. They must train library staff regarding DISM because large numbers of libraries have DISM policies but have failed to implement them.
- Libraries should adopt the DISM policy and IT infrastructure with the latest tools to protect confidential and sensitive data.
- Academic libraries should adopt documented policies, guidelines for data protection, sharing confidential information, system usage and technical aspects. Policies should focus on information system security, cyber security, system implementation and intellectual property.
- Digital libraries should establish a strong DISM policy to protect organisational and technological measures that were very poor, including policies on digital contents, network, IT infrastructure, backup data, hardware and software. Libraries must have policies on data privacy, data protection, new technology adoption and privacy disasters.
- Policies and procedures must be developed and implemented for digital libraries to protect the digital data assets, protect the data and back up the data. Privacy and confidentiality must be ensured by the libraries.
- Library professionals should train themselves because some librarians have less knowledge, awareness and training on DISM. Librarians might be trained to secure digital content and data.
- Libraries must adopt and implement DISM policies for user benefit and patron trust. Policies must be implemented to protect the privacy of users' data, sensitive information and user trust. Libraries must conduct training courses for librarians and users. Librarians must be aware of how to protect user data. 'There is no excuse for librarians to get it wrong because their whole training and ethos is about managing information properly' [54].
- Libraries should develop and implement policies, guidelines and procedures for librarians regarding data protection, sharing confidential information, system usage as a user's, digital contents, network infrastructure, IT infrastructure, backup data, hardware and software.
- Libraries must train staff and users regarding DISM. There should be trained DISM staff in libraries. The policy also ensures that the data, staff and organisation are protected. The policy also educates the librarian, libraries and IT professionals on how to save the data.

### *Contribution/implications*

Libraries promote research culture in this digital and developed world by providing resources to users for educational and research purposes. Moreover, in developing countries, library professionals faced challenges in developing and implementing the DISM policy. The awareness, knowledge and culture of DISM and DISM policy must be promoted in libraries. To protect data privacy and security, library professionals, administrators and stakeholders promote and implement the DISM policy in their libraries and organisations. This study is beneficial for library professionals, administrators, policymakers and management to make DISM policies and implement them in their organisation or libraries to secure sensitive, personal data and resources.

### *Future research and gap*

- There is dearth of international literature on DISM in the field of libraries, and there is need to conduct more studies on DISM phenomenon.
- There is limited literature available on DISM policy in academic libraries, so research should be conducted on DISM policy in academic libraries in developing countries.

- There is limited literature and frameworks available on DISM policy about hardware, software, infrastructure, data protection, privacy, backup, retrieval and dissemination.
- There is also a need to work on the DISM policy on protection from viruses, social engineering, hacker attacks and others.
- There is a need for DISM awareness, training, knowledge, and the making and implementation of the policy in academic libraries.


### Declaration of conflicting interests


The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

### Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

### ORCID iDs

Ghulam Farid  <https://orcid.org/0000-0002-3299-5220>

Nosheen Fatima Warraich  <https://orcid.org/0000-0002-1901-9743>

### Supplemental material

Supplemental material for this article is available online.

### References

- [1] Ansari MN. ICT skills proficiency of library professionals: a case study of universities in Karachi, Pakistan. *Chin Librariansh* 2013; 36(1): 72–84.
- [2] Abelein U and Paech B. Understanding the influence of user participation and involvement on system success – a systematic mapping study. *Empir Softw Eng* 2015; 20: 28–81.
- [3] Ifijeh G. Adoption of digital preservation methods for theses in Nigerian academic libraries: applications and implications. *J Acad Librariansh* 2014; 40(3–4): 399–404.
- [4] Mavodza J. The impact of cloud computing on the future of academic library practices and services. *New Libr World* 2013; 114(3/4): 132–141.
- [5] Ali RF, Dominic PD, Ali SE et al. Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. *Appl Sci* 2021; 11(8): 3383.
- [6] Aslam M, Khalid A, Batool SH et al. Mapping digital information security management in the university libraries of Pakistan. *Proc Assoc Inf Sci Technol* 2019; 56(1): 356–359.
- [7] Singh V and Margam M. Information security measures of libraries of Central Universities of Delhi: a study. *DESIDOC J Lib Inf Technol* 2018; 38(2): 102–109.
- [8] Al-Dhahri S, Al-Sarti M and Abdul A. Information security management system. *Int J Comput Appl* 2017; 158(7): 29–33.
- [9] Bolten JB. Executive office of the president (Director), 2003, <http://www.regulationwriters.com/downloads/eGov-ImplementationM03-18.pdf>
- [10] Stevens G. *Federal information security and data breach notification laws*. Collingdale, PA: DIANE Publishing, 2010.
- [11] Shivarama J, Dawar MV and JVPDS VW. Comparative study of information security management models for academic libraries in digital environment. In: *Future librarianship: innovative embedded, sustainable and emerging trends-international conference*, ISKCOM <https://iskcom.nmims.edu/about-iskcom.php> (2016, accessed November 11 2016).
- [12] Astakhova LV. Issues of the culture of information security under the conditions of the digital economy. *Sci Tech Inf Process* 2020; 47: 56–64.
- [13] ISOJ. *ISO/IEC 27000: 2012, information technology – security techniques – information security management systems – overview and vocabulary*. Geneva: International Organization for Standardization, 2012.
- [14] Schweizerische SN. Information technology – security techniques – information security management systems – requirements. *ISO/IEC International Standards Organization*, <https://eldritchdata.neocities.org/PDF/CS/SecManagmentSystemsReq.pdf> (2013, accessed October 2 2019).
- [15] Morgan S. Cybersecurity business report. <https://www.csoonline.com/in/blog/cybersecurity-business-report/>
- [16] Aithen R. Global information security spending to exceed \$124B in 2019, privacy concerns driving demand. *Forbes*, 9 August 2018, <https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/?sh=a69d37271128>
- [17] Whitman ME and Mattord HJ. *Principles of information security*. Boston, MA: Cengage learning, 2021.

- [18] Smith S, Winchester D, Bunker D et al. Circuits of power: a study of mandated compliance to an information systems security 'De Jure' standard in a government organization. *MIS Quarterly* 2010; 34: 463–486.
- [19] Niemimaa E and Niemimaa M. Information systems security policy implementation in practice: from best practices to situated practices. *Eur J Inf Syst* 2017; 26(1): 1–20.
- [20] Andersson A, Hedström K and Karlsson F. Standardizing information security – a structural analysis. *Inf Manag* 2022; 59(3): 103623.
- [21] Disterer G. ISO/IEC 27000, 27001 and 27002 for information security management. *J Inf Secur* 2013;4(2): 92–100.
- [22] Soliman, W., & Mohammadnazar, H. (2022). New Insights into the Justifiability of Organizational Information Security Policy Noncompliance : A Case Study. In *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS 2022)* (pp. 6812–6821). University of Hawai'i at Manoa. Proceedings of the Annual Hawaii International Conference on System Sciences. <https://doi.org/10.24251/HICSS.2022.823>.
- [23] Chen H and Li W. Understanding organization employees information security omission behavior: an integrated model of social norm and deterrence. In: *Proceedings 18th Pacific Asia Conference on Information Systems, PACIS 2014*, Chengdu, China, June 24-28, 2014, <https://researchr.org/publication/pacis-2014>.
- [24] Flowerday SV and Tuyikeze T. Information security policy development and implementation: the what, how and who. *Comput Secur* 2016; 61: 169–183.
- [25] Agboola B and Aduku BS. Managing security issues in Federal University Gashua Library, Yobe State, North East of Nigeria. In: *Proceedings of 1st conference on personal security and community policing*, 2019. pp. 1–10. Katsina State, Nigeria: Alqalam University.
- [26] Johnson P. *Fundamentals of collection development and management*. American Library Association, 2018, [https://www.ala-tore.org/sites/default/files/book\\_samples/9780838916414\\_sample.pdf](https://www.ala-tore.org/sites/default/files/book_samples/9780838916414_sample.pdf)
- [27] Hao T. The information security analysis of digital library. In: *2015 8th international conference on intelligent computation technology and automation (ICICTA)*, Nanchang, China, 14–15 June 2015, pp. 983–984. New York: IEEE.
- [28] Han Z, Huang S, Li H et al. Risk assessment of digital library information security: a case study. *Electron Lib* 2016; 34(3): 471–487.
- [29] Fox E and ElSherbiny N. *Security and digital libraries, digital libraries – methods and applications*. London: Intech, 2011.
- [30] Ismail R and Zainab AN. Assessing the status of library information systems security. *J Librariansh Inf Sci* 2013; 45(3): 232–247.
- [31] Olajide O. Theft and mutilation challenges and management in academic libraries: a case study of Federal University Oye-Ekiti, Nigeria. *J Appl Inf Sci Technol* 2017; 10(1): 78–84.
- [32] Merchan-Lima J, Astudillo-Salinas F, Tello-Oquendo L et al. Information security management frameworks and strategies in higher education institutions: a systematic review. *Ann Telecom* 2021; 76: 255–270.
- [33] Anday A, Francese E, Hurdeman HC et al. Information security issues in a digital library environment: a literature review. *Bilgi Dünyası* 2012; 13(1): 117–137.
- [34] Osayande O. Electronic security systems in academic libraries: a case study of three university libraries in South-West Nigeria. *Chin Librariansh* 2011; 32: 1–10.
- [35] Hussain A and Abalkhail AM. Determinants of library use, collections and services among the students of engineering: a case study of King Saud University. *Coll Build* 2013; 32(3): 100–110.
- [36] Jones BM. Libraries, technology, and the culture of privacy a global perspective. *Lib Technol Rep* 2010; 46(8): 8–12.
- [37] Zimmer M. Patron privacy in the '2.0' era: avoiding the Faustian bargain of library 2.0. *J Inf Ethic* 2013; 22(1): 44.
- [38] Hampwaye B. *Assessment of the security systems in selected libraries of higher learning institutions in Zambia*. Doctoral dissertation, University of Zambia, Lusaka, Zambia, 2022.
- [39] Vyas PR and Pathak SR. Theft and mutilation of library resources in University Libraries of India. *Lib Philos Pract*. <https://digitalcommons.unl.edu/libphilprac/4371>. (accessed October 5 2020).
- [40] Kuzma J. European digital libraries: web security vulnerabilities. *Lib Hi Tech* 2010; 28(3): 402–413.
- [41] Almasalha HM, Taha NN and Abumqibl A. The status quo of information security from the perspective of information technology staff in Jordanian University Libraries. *J Inf Secur Cybercrimes Res* 2021; 4(1): 55–80.
- [42] Moher D, Shamseer L, Clarke M et al. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Syst Rev* 2015; 4(1): 1–9.
- [43] Bearman M, Smith CD, Carbone A et al. Systematic review methodology in higher education. *High Educ Res Dev* 2012; 31(5): 625–640.
- [44] Wang H. Research and implementation of security policy of library digital information. In: *2013 International Conference on Advances in Social Science, Humanities, and Management (ASSHM-13)*, Guangzhou, China, 14–15 December 2013, pp. 564–570. Paris: Atlantis Press.
- [45] Yamson GC and Cobblah M. Assessments of collection security management in academic libraries: a case study of Central University Library. In: *5th Eurasian Multidisciplinary Forum, EMF*, Tbilisi, 27–28 October 2016.
- [46] Khan A, Ibrahim M and Hussain A. An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *Int J Inf Manag Data Insights* 2021; 1(2): 100015.

- [47] Maidabino AA and Ngah ZA. Collection security issues in Malaysian academic libraries: an exploratory survey. *Lib Philos Pract* 2010; 1–1.
- [48] Ali SM. Integration of information security essential controls into information technology infrastructure library-a proposed framework. *Int J Appl* 2014; 4(1):95–100.
- [49] Abioye A and Adeowu OF. Security risks management in selected academic libraries in Osun State, Nigeria. *Inf Manager* 2013; 13(1–2): 1–9.
- [50] Zaveri P. Digital disaster management in libraries in India. *Lib Hi Tech* 2015; 33(2): 230–244.
- [51] Chowdhury G. Sustainability of digital libraries: a conceptual model and a research framework. *Int J Digit Lib* 2014; 14: 181–195.
- [52] Gressel M. Are libraries doing enough to safeguard their patrons' digital privacy? *Ser Lib* 2014; 67(2): 137–142.
- [53] Hess AN, LaPorte-Fiori R and Engwall K. Preserving patron privacy in the 21st century academic library. *J Acad Lib* 2015; 41(1): 105–114.
- [54] Sutlieff L and Chelin J. 'An absolute prerequisite': the importance of user privacy and trust in maintaining academic freedom at the library. *J Lib Inf Sci* 2010; 42(3): 163–177.
- [55] San Nicolas-Rocca T and Burkhard RJ. Information security in libraries. *Inf Technol Lib* 2019; 38(2): 58–71.
- [56] Al-Ameen MN, Tamanna T, Nandy S et al. We don't give a second thought before providing our information: understanding users' perceptions of information collection by apps in Urban Bangladesh. In: *Proceedings of the 3rd ACM SIGCAS conference on computing and sustainable societies*, Guayaquil, Ecuador, 15–17 June 2020.
- [57] Al-Suqri MN and Akomolafe-Fatuyi E. Security and privacy in digital libraries: challenges, opportunities and prospects. *Int J Digit Lib Syst (IJDLIS)* 2012; 3(4): 54–61.
- [58] He W, Yuan X and Yang L. Supporting case-based learning in information security with web-based technology. *J Inf Syst Educ* 2013; 24(1): 31.
- [59] Amini M, VakiliMofrad H and Saberi MK. Designing and psychometric evaluation of questionnaire of human factors affecting information security in libraries. *Lib Philos Pract* 2020; 2020: 1–9.
- [60] Yeboah EB, Kwafoa P and Amoah GB. Security of staff in academic libraries: a study of Sam Jonah Library, University of Cape Coast, 2017. <http://www.publishingindia.com/jais/71/security-of-staff-in-academic-libraries-a-study-of-sam-jonah-library-university-of-cape-coast/619/4384/>
- [61] Fakeh SK, Zulhemay MN, Shahibi MS et al. Information security awareness amongst academic librarians. *J Appl Sci Res* 2012; 8(3): 1723–1735.
- [62] Segurança da Informação em Bibliotecas Universitárias. Information security in academic libraries: the role of the librarian in planning and introducing new institutional policies. *Digit J Lib Inf Sci* 2017; 15(2): 389–419.
- [63] Abduldayan FJ, Fasola A, Oyedum GU et al. Research data management and information security: role of library and information technology service (ITS) units in federal universities of technology in Nigeria. *I-Manager J Inf Tech* 2018; 8: 20–28.
- [64] Wu Z, Shen S, Li H et al. A comprehensive study to the protection of digital library readers' privacy under an untrusted network environment. *Lib Hi Tech* 2022; 40(6): 1930–1953.