

# Information Resources Security Management for Improved Service Delivery in Public University Libraries in Kano State

Safiyya Umar Babba<sup>1,\*</sup>, Abbas Atiku Mai-dabino, PhD<sup>2</sup>

<sup>1</sup> Department of Library and Information Sciences, Bayero University Kano, Kano State, Nigeria

<sup>2</sup> Federal University of Health Sciences, Babura, Jigawa State, Nigeria

\* Corresponding author: safiyaumar292@gmail.com

| ARTICLE HISTORY                                                                 | ARTICLE INFO                                                                                                                              | HOW TO CITE                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Received: 11 July 2026<br>Accepted: 5 September 2026<br>Published: October 2026 | Vol. 1, No. 1 (2026), pp. 227–238<br>ISSN: 3141-6268 (Print)<br>3156-5077 (Online)<br>DOI: 10.67523/aujmss.v1i1.022<br>License: CC BY 4.0 | Babba, S. U., & Mai-dabino, A. A. (2026). Information resources security management for improved service delivery in public university libraries in Kano State. <i>Azman Univ. Int. J. Manag. Soc. Sci.</i> , 1(1), 227–238.<br><a href="https://doi.org/10.67523/aujmss.v1i1.022">https://doi.org/10.67523/aujmss.v1i1.022</a> |

## ABSTRACT

This study investigated information resources security management in public university libraries in Kano State. The study sought to address the following research objectives: to find out the types of security issues university libraries in Kano State faced and to identify the security methods used for collection protection in university libraries in Kano State. The study adopted a qualitative descriptive design and used thematic analysis. Twelve participants formed the sample, purposive sampling was used in selecting participants from public universities in Kano including Bayero University, North West University, Aliko Dangote University of Science and Technology and Police Academy, Wudil. Participants were selected for the study because they are part of senior management and based on their experience, knowledge and work roles. All the participants of the study had been coded as P1-P12 to ensure anonymity of conducting and reporting the interview in line with ethical requirements of qualitative research. An interview guide was used as the research instrument. The findings revealed that mutilation, theft, hiding books in bags was among the types of collection security issues in their libraries. The findings of the study revealed that library personnel, CCTV were among the method used for collection protection in their libraries. The researcher recommended that the university libraries should endeavor to have a comprehensive library security policy which stipulates rules, procedures and sanctions for library users and library staff.

**Keywords:** University Libraries; Security Issues; Security Methods Used; Library Collection Protection

## **1.0 Introduction**

Libraries are central to the academic reputation of institutions as they support teaching, learning and research. They are known to protect and house physical and digital resources, including rare manuscripts, academic journals, and electronic databases, which are essential for education and research. In Nigeria, where funding for library acquisitions is often limited, the loss of these resources through theft or mutilation can severely hamper academic progress (Igbinovia & Ishola, 2023). This is evident in their role in providing adequate security measures, such as RFID systems and CCTV, to deter such losses and ensure continued access to knowledge.

Library security refers to the comprehensive set of measures, policies, and technologies implemented to protect library resources, facilities, and users from threats such as theft, mutilation, vandalism, unauthorised access, and digital breaches. According to Igbinovia and Ishola (2023), library security encompasses ensuring the safety of information resources in the digital realm and addressing risks such as cyberattacks and data breaches, which are increasingly prevalent in academic libraries. Additionally, library security involves creating a safe environment for users and staff, striking a balance between accessibility and protection to maintain the library's role as a trusted academic hub (Olajide, 2017).

Some materials in university libraries contain information of cultural value; consequently, they must be safeguarded for current and upcoming generations. University library resources must be well secured from misuse, defacing, theft, and mutilation. The deliberate cutting off, removal of parts, or damage to library materials to deny access to other users constitutes mutilation (Omoike & Alabi, 2020). The destruction of library materials, the tearing of relevant pages, and the writing of unpalatable things in the materials posed threats to the efficient operation of the library. It also imposes financial burdens on the library management since they have to replace the lost materials with their already shrinking budget allocation.

According to Osayande (2019), the purpose of using collection security systems must be to create secure surroundings for staff in the library, items, and customers. The author added that it is also crucial to make sure that security procedures are carried out as smoothly as possible, without obstructing the library's goal of creating a welcoming environment. Osayande (2019) came to the conclusion that security problems have always plagued libraries. Materials that are taken from libraries or damaged make challenging replacements since they may be out of print or the library may not have the funds to buy a new copy. Manually inspecting customers' baggage, the old-fashioned approach is both ineffective and unfriendly. Adopting electronic security systems is a superior strategy for handling security in libraries. This will increase the effectiveness of protecting library materials from theft, mutilation, and other types of criminal activity.

Universities in Kano consist of public and private, which are established and managed by the State, private and federal, which are owned by entities. They have missions of creating and transferring knowledge in State and beyond. As a result, the university libraries in Kano State have a vast range of collections to support their missions. These collections include print, electronic and non-print resources. The collections are very important to support the activities in the academic environments such as teaching, learning and research. On this note the researcher investigated information resources security management in university libraries in Kano State.

## **1.2 Statement of the Problem**

The library organises information resources and provides services to users to suit their information needs as students, professors, and members of the university community. Despite librarians' efforts to satisfy users' information demands, they confront persistent problems in providing information services, including missing items and damage caused to library resources by deviant users. Theft, mutilation, and misuse of library and information resources are common examples of such delinquent behavior. Ofori et al. (2022) identified unsecured windows, faulty emergency exits, insufficient staff in the computer room, and inadequate policies and procedures as motivational factors behind theft, mutilation, and offensive acts in libraries. They also pointed to a lack of security plans and inadequate security points, including exits, loading areas, windows, special collections, short renewal intervals, and inadequate signage. Mindapa (2022) noted that these practices prevent other potential users from making full use of information resources.

Existing empirical work on this problem, however, has concentrated on institutions outside Kano State. Omoike and Alabi (2020) examined theft, mutilation, and vandalism at the University of Ibadan; Chinwendu (2019) studied an academic library in Lagos State; Elizabeth and Ogunjimi (2019) focused on university libraries in Southwest Nigeria; and Oladapo and Yusuf (2022) surveyed polytechnic libraries using a quantitative Likert-scale instrument. Public university libraries in Kano State operate under a different institutional and resource environment, and no identified study has examined how library personnel in these specific institutions experience and respond to collection security threats, nor has the security experience of these libraries been captured through the accounts of the personnel directly responsible for circulation and collection protection. This contextual gap leaves university library management in Kano State without evidence specific to their own institutions on which to base security decisions.

The present study therefore investigated information resources security management in public university libraries in Kano State, with two objectives: to identify the types of collection security issues these libraries face, and to identify the security methods used for collection protection. Correspondingly, the study sought to answer what types of collection security issues are faced in university libraries in Kano State, and what security methods are used for collection protection in these libraries. The study was confined to the public university libraries in Kano State, namely Bayero University (BUK), North West University (NWU), Aliko Dangote University of Science and Technology, Wudil (ADUST), and the Police Academy, Wudil (POLAC), and examined the security issues these libraries face alongside the measures currently in place to address them.

Findings from the study are intended to give university library managers in Kano State institution-specific evidence on which to base security decisions, something the studies conducted elsewhere cannot supply. The absence of a documented security policy in most of the universities under study means the findings can inform the development of such a policy directly, rather than through evidence drawn from a different institutional context. The study also extends the empirical record on library security in Nigeria to a setting, public universities in Kano State, that has not previously been examined, and its findings may be of use to bodies such as the Librarian Registration Council of Nigeria (LRCN) and the National Library Association (NLA) in setting sector-wide security guidance.

## **2.0 Literature Review**

### **2.1 Types of Security Issues in University Libraries**

Empirical accounts of library security threats converge on a small set of recurring problems: theft, mutilation, and vandalism of collections. Studies conducted across different Nigerian contexts, including the University of Ibadan (Omoike & Alabi, 2020), an academic library in Lagos State (Chinwendu, 2019), and university libraries in Southwest Nigeria (Elizabeth & Ogunjimi, 2019), report a consistent pattern: high rates of theft and damage, concealment of books to restrict other users' access, and deliberate defacement of materials. What varies across these studies is less the nature

of the threat than the conditions under which it occurs. Chinwendu (2019) traces the problem partly to inadequate photocopying facilities and the high cost of reading materials, which push users toward removing or damaging materials rather than reproducing them legitimately, while also identifying a failure of library staff to monitor user behavior as a contributing factor. Ofori et al. (2022) locate the problem further upstream, in structural and procedural weaknesses, unsecured windows, faulty emergency exits, insufficient staffing in computer rooms, inadequate policies, and poor signage around exits and special collections, that create the physical opportunity for theft and mutilation rather than causing it directly.

Read together, these studies suggest collection security threats in Nigerian university libraries arise from an interaction between user motivation (cost pressures, opportunism) and institutional gaps (weak surveillance, poor infrastructure, absent policy), rather than from either factor alone. What remains less clear from this literature is how these threats manifest in the day-to-day accounts of the personnel directly responsible for circulation and monitoring, since the studies cited rely primarily on incidence data and staff-level structural assessments rather than the operational perspective of frontline library staff, a gap the qualitative approach of the present study is positioned to address in the context of Kano State.

## **2.2 Security Methods used for Collection Protection in University Libraries**

The methods reported in the literature fall broadly into two categories: personnel-based vigilance and technological or procedural controls, and the evidence suggests the two are treated as complementary rather than substitutable. Agboola and Aduku (2019) describe periodic staff movement through the library floor as a low-cost deterrent to theft and mutilation, alongside exit points, physical body searches, and permanent security personnel at entrances, measures the authors frame as necessary even where surveillance cameras are already installed. Basaka et al. (2020) document a parallel institutional response at Abubakar Tafawa Balewa University, where recurring theft involving students and staff led to the introduction of identification cards specifically to strengthen monitoring of who accesses the collection, illustrating how a documented breach pattern can drive adoption of a specific control. Gupta and Madhusudhan (2021) shift the emphasis toward electronic security systems, arguing that adopting such measures reduces theft, mutilation, and improper shelving, a claim consistent with the view that procedural remedies alone (staff movement, ID checks) are not sufficient once a library's collection and user base reach a certain scale.

The clearest empirical test of relative effectiveness comes from Oladapo and Yusuf (2022), whose survey of fifty librarians in Nigerian polytechnic libraries found physical measures such as locks and guards only moderately effective ( $M = 2.64$ ), with vulnerabilities increasing in the absence of CCTV. This finding qualifies the more general claims in the earlier studies: personnel-based and procedural measures appear necessary but not sufficient, and their effectiveness declines without a technological layer. However, Oladapo and Yusuf's survey design, while allowing broader coverage than a single-institution case study, cannot capture the reasoning library personnel give for why certain methods are adopted over others or how these methods function in practice, a limitation the present study's qualitative design is intended to address for the Kano State context.

### **2.3 Theoretical Framework**

The study adopted the House Security Management Model, an operational model proposed by Maidabino (2016) for understanding collection security governance in libraries. The model's central proposition is that collection security in a library functions the way security functions in a house: a house may be fitted with locks and an alarm system, but its overall security still depends on whether the occupants consistently use those systems, for example, locking the front entrance, rather than on the presence of the systems alone. Applied to a library, the model holds that collection security is not reducible to the presence of any single measure, whether a policy document, a surveillance camera, or a security guard, but is instead the joint product of five interacting factors: governance (the existence and enforcement of security policy), operational processes (the day-to-day procedures for monitoring circulation, exits, and access points), people awareness and training (the extent to which staff and users understand and apply security procedures), physical and technological measures (locks, CCTV, identification systems, and similar controls), and security culture (the shared behavioral norms that determine whether the other four factors are actually observed in practice).

The model's key assumption, carried directly from its house metaphor, is that these five factors are interdependent rather than additive: a weakness in one factor, most importantly security culture, can undermine the protective value of strength in the others. A library with CCTV, access-controlled entry points, and a written security policy can still experience high rates of theft and mutilation if staff do not consistently apply monitoring procedures or if users are not deterred by measures they know are inconsistently enforced. This assumption makes the model appropriate for the present study because the research problem, as established in the empirical literature reviewed in Sections 2.1 and 2.2, is not the absence of security measures in Nigerian university libraries but their uneven and often informal application, a pattern the model is specifically built to explain.

The five factors map onto the study's two constructs as follows. The types of collection security issues examined under the first objective, theft, mutilation, concealment, impersonation, and non-return of materials, correspond to breakdowns in operational processes, security culture, or both, since each represents a point at which an existing or intended control failed to prevent the behavior. The security methods examined under the second objective, personnel monitoring, CCTV, and access control, correspond to physical and technological measures and operational processes, while the extent to which these methods are formalized, or left to informal staff vigilance as several participant accounts suggest, speaks to the governance and security-culture factors. The model is used here in an applying rather than extending capacity: the study does not modify the model's five factors but uses them as an interpretive lens for organizing findings that would otherwise remain a flat list of issues and methods, allowing the Discussion to explain not only what security problems and methods were reported but why certain methods may be present without eliminating the issues they were intended to address.

One limitation of the model, noted here rather than in the Limitations section since it concerns the theoretical lens rather than the study's own design, is that it was developed as a general operational framework and has not been extensively validated through qualitative fieldwork of the kind conducted here; the present study therefore also serves as an empirical application of the model to a qualitative, single-country context in which it has seen limited prior testing.

### **3.0 Research Methodology**

The study adopted a qualitative descriptive design, with thematic analysis used as the principal analytic approach. This design was considered appropriate because the study sought to obtain and describe participants' accounts of information-resource security issues and the methods used for collection protection, rather than to reconstruct or interpret individual life stories. The design therefore enabled the researcher to present participants' experiences and views in a clear, context-sensitive manner while retaining the language and meanings expressed during the interviews. The study comprised exactly twelve (12) participants, drawn from the four public university libraries covered by the study, Bayero University (BUK), North West University (NWU), Aliko Dangote University of Science and Technology, Wudil (ADUST), and the Police Academy (POLAC). At each of the four institutions, three librarians participated: the head of the circulation unit and two academic librarians. Thus, the total sample was 12 librarians (3 participants  $\times$  4 institutions), identified as P1–P12 in the findings. Purposive sampling was used in selecting the participants because these participants were directly involved in circulation activities and were considered knowledgeable about information-resource security practices. Data were collected through a semi-structured interview guide.

#### **3.1 Data Collection and Preparation**

The interview guide was organised around the two research objectives, focusing on the types of collection security issues experienced in the libraries and the methods used to protect information resources. Interview guide was open ended questions, each interview guide was sent to the participant through the help of research assistance in those university libraries. Personal identifiers were removed from the transcripts and participants were assigned codes P1–P12.

#### **3.2 Data Analysis Procedure**

The interview data were analysed using thematic analysis, consistent with the qualitative descriptive design, following the sequence of familiarization, coding, theme searching, theme review, and theme definition. The researcher first became familiar with the data by repeatedly reading the transcripts and field notes to gain an overall sense of the accounts provided by participants. Initial codes were then generated by systematically labelling recurring words, phrases, and ideas across the twelve transcripts, for example, references to CCTV, staff movement, book concealment, or non-return of materials, without yet grouping them into broader categories. These initial codes were subsequently sorted into candidate themes by grouping codes that reflected a shared underlying issue or method, such as combining references to hiding books in bags and concealing books in clothing under a single concealment-related theme. Candidate themes were then reviewed against the coded extracts and the full data set to check that each theme was supported by sufficient and consistent evidence and that no theme merely repeated another under a different label; themes that overlapped too closely were merged, while those with too little supporting data were reconsidered. Once the candidate themes were confirmed, each was clearly defined and named to capture its specific scope, resulting in the four security-issue themes and three security-method themes presented in Tables 1 and 2. Finally, the themes were interpreted descriptively in relation to the two research objectives and presented using concise narrative summaries and selected verbatim quotations from participants, reported using codes (P1–P12) to preserve anonymity. Because the study was qualitative descriptive rather than narrative inquiry, the analysis did not treat storyline, chronological sequence, or individual life-story structure as analytic units.

### 3.3 Trustworthiness of the Study

Trustworthiness was addressed through credibility, dependability, confirmability and transferability. Credibility was enhanced by purposively selecting participants who had direct knowledge and experience of circulation and collection-security activities, using a semi-structured interview guide aligned with the research objectives, and comparing participants' responses across the four libraries. The researcher also maintained close engagement with the interview data during transcription, coding and theme development. Dependability was promoted by maintaining a clear record of the data-collection and analysis procedures, including the interview guide, participant selection process, transcription, coding and development of themes. Confirmability was strengthened by grounding interpretations in participants' actual statements and retaining an audit trail of coding decisions so that findings could be traced back to the interview data. Transferability was supported by providing a clear description of the study setting, participants, sampling procedure and data-collection process, enabling readers to judge the applicability of the findings to similar university-library contexts.

### 3.4 Ethical Approval and Informed Consent

Ethical principles were observed throughout the study. Before data collection, permission to conduct the study was obtained from the relevant institutional authorities of the participating university libraries, and the study was conducted in accordance with applicable institutional research-ethics requirements. Participants were informed about the purpose of the study, what participation involved, the voluntary nature of participation, and their right to decline to answer any question or withdraw without penalty. Informed consent was obtained before the interviews were conducted. Participants' identities were protected by using participant codes (P1–P12) in the presentation of findings, and the information obtained was used solely for academic research purposes. No participant was identified by name in the report.

## 4.0 Results and Discussions

Participants were asked about the types of collection security issues in their library.

**Table 1: Types of Collection Security Issues in University Libraries (n = 12)**

| Theme                                              | Description                                          | Representative Participant Codes | Illustrative Quotation                                            |
|----------------------------------------------------|------------------------------------------------------|----------------------------------|-------------------------------------------------------------------|
| Unauthorized removal and physical damage           | Theft or destruction of materials and equipment      | P1, P2, P3, P10                  | "Theft, mutilation, stealing of computer adapters and mouse" (P3) |
| Concealment and circumvention of physical controls | Users hiding or smuggling materials past checkpoints | P4, P6, P7, P8, P11              | "Concealing books in clothes" (P8)                                |
| Circulation-stage breaches                         | Failure to return borrowed materials                 | P9                               | "Non-return of borrowed books" (P9)                               |
| Identity and access-control breaches               | Impersonation or bypassing entry controls            | P5, P12                          | "Unauthorized access" (P12)                                       |

The following are some of the direct quotations from the participants.

*P1 "Mutilation and theft"*

*P2 "High level of mutilation of books"*

*P3 "Theft, mutilation, stealing of computer adopters and mouse"*

*P4 "Hiding books in bags"*

*P5 "Impersonation"*

*P6 “Throwing books through windows”*

*P7 “Evading security checks”*

*P8 “Concealing books in clothes”*

*P9 “Non-return of borrowed books”*

*P10 “Theft and vandalization of printed material”*

*P11 “Evading security checks and Theft”*

*P12 “Unauthorized access”*

As shown in Table 1, the collection-security problems reported by participants fall into four themes: unauthorized removal and physical damage, concealment and circumvention of physical controls, circulation-stage breaches, and identity and access-control breaches. The accounts suggest these problems arise where users can exploit gaps between circulation procedures, physical surveillance, and exit controls. Unauthorized removal and physical damage, covering theft, mutilation, and the loss of equipment such as computer adapters and mice, represented the most frequently reported theme. Concealment and circumvention of physical controls, hiding books in bags or clothing, throwing books through windows, and evading security checks, point to deliberate attempts to bypass existing checkpoints rather than exploit their absence. Circulation-stage breaches, represented by the non-return of borrowed books, indicate a distinct point of weakness that occurs after the initial borrowing transaction rather than at a physical checkpoint. Identity and access-control breaches, impersonation and unauthorized access, similarly point to risks specific to user identification rather than to physical concealment or delayed return.

Objective two of the study sought to find out the security methods used for collection protection in university libraries. The participants were asked to indicate the method they took to secure information resources in their library.

**Table 2: Security Methods Used for Collection Protection (n = 12)**

| Theme                      | Description                                               | Representative Participant Codes | Illustrative Quotation                                                     |
|----------------------------|-----------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------|
| Electronic surveillance    | CCTV installation and monitoring                          | P2, P3, P4, P6, P11, P12         | "Installation of CCTV camera" (P4)                                         |
| Personnel-based monitoring | Security or library staff patrolling and observing users  | P1, P5, P7, P8, P9, P12          | "Security personnel moving around in the library" (P8)                     |
| Access control             | Identity verification and security guards at entry points | P10, P11                         | "Checking identity cards allowing access, and using security guards" (P10) |

The following are some of the direct quotations from the participants.

*P1 “By monitoring library users”*

*P2 “By using CCTV camera and many more”*

*P3 “We used CCTV cameras in our university”*

*P4 “Installation of CCTV camera”*

*P5 “Steady checking of the library users”*

*P6 “By providing security personnel and mounting of CCTV”*

*P7 “Personnel moving around in the library”*

*P8 “Security personnel moving around in the library”*

*P9 “Monitoring users at the circulation desk”*

*P10 “Checking identity cards allowing access, and using security guards”*

*P11 “CCTV Installation and proper checking of users”*

#### *P12 “Observing, monitoring, checking and CCTV installation”*

As shown in Table 2, the methods participants described for collection protection group into three themes: electronic surveillance, personnel-based monitoring, and access control. Electronic surveillance, primarily CCTV installation and monitoring, was the most frequently cited method across the libraries studied. Personnel-based monitoring, security or library staff observing users and moving through the library floor, including at the circulation desk, was reported almost as frequently, often alongside electronic surveillance rather than in place of it. Access control, checking identity cards and the use of security guards at entry points, was the least frequently reported of the three themes, suggesting it may be the least consistently applied method across the libraries under study.

### **4.1 Discussion of Findings**

#### **Types of Security Issues Facing the University Libraries**

The four themes identified in Table 1, unauthorized removal and physical damage, concealment and circumvention of physical controls, circulation-stage breaches, and identity and access-control breaches, correspond most directly to breakdowns in operational processes and security culture within the House Security Management Model. Unauthorized removal and physical damage (P1, P2, P3, P10) and concealment behaviors such as hiding books in bags or clothes (P4, P6, P7, P8, P11) both point to gaps in the day-to-day monitoring procedures that the model locates under operational processes: these are precisely the kinds of opportunities that arise when circulation checks, exit surveillance, or bag inspection are inconsistently applied rather than absent altogether. This pattern is consistent with Omoike and Alabi (2020), who identified theft, mutilation, and vandalism as recurring threats at the University of Ibadan, and with Chinwendu (2019), whose finding of a high rate of theft and damage was attributed partly to a failure of staff to monitor user behavior, an operational rather than a purely technological failure.

The circulation-stage breach identified here, non-return of borrowed books (P9), sits somewhat apart from the other themes because it occurs after the point of physical control rather than at it, implicating governance, specifically whether clear policy and enforceable sanctions exist for overdue or unreturned materials, more than physical surveillance. Similarly, the identity and access-control breaches captured in impersonation and unauthorized access (P5, P12) reflect a people awareness and training gap as much as a procedural one: these behaviors depend on staff either failing to verify identity consistently or lacking a clear procedure to do so. Elizabeth and Ogunjimi (2019) reported comparable instances of theft, mutilation, and deliberate concealment in Southwest Nigerian university libraries, suggesting these are not issues specific to the institutions studied here but a broader pattern across Nigerian public university libraries in which no single factor in the model, whether governance, process, or culture, is fully absent, but none is consistently strong enough to close the gaps the others leave open.

### **Security Methods used for Collection Protection**

The three methods identified in Table 2, electronic surveillance, personnel-based monitoring, and access control, map more directly onto the model's physical and technological measures and operational processes factors than the security issues did, which is expected since these are the deliberate controls libraries have put in place in response to the problems discussed above. Electronic surveillance, primarily CCTV (P2, P3, P4, P6, P11, P12), was the most frequently cited method among participants, echoing Gupta and Madhusudhan's (2021) finding that adopting new security measures, particularly electronic ones, contributes to reducing theft, mutilation, and improper shelving. Personnel-based monitoring, security or library staff moving through and observing the library floor (P1, P5, P7, P8, P9, P12), was reported almost as frequently and corresponds to Agboola and Aduku's (2019) recommendation that periodic staff movement remain a priority even where surveillance cameras are already installed, a point the present findings support directly since several participants named both CCTV and personnel monitoring as methods used in the same library.

The reliance on personnel-based monitoring alongside, rather than instead of, electronic surveillance is consistent with the model's assumption that physical and technological measures alone are insufficient without an accompanying operational and cultural commitment to using them: a camera system does not enforce itself, and the presence of staff moving through the collection reflects an attempt to maintain the security culture factor that the model treats as necessary for the other measures to function as intended. This reading is supported by Oladapo and Yusuf (2022), who found physical measures such as locks and guards only moderately effective ( $M = 2.64$ ) and vulnerabilities increasing specifically in the absence of CCTV, indicating that no single factor, personnel or technology, is sufficient on its own. Access control through identity verification and security guards at entry points (P10, P11) reflects the governance factor most directly among the three methods, since it depends on an institutional decision to require and enforce identity checks rather than on staff vigilance in the moment; its comparatively lower frequency among participant responses suggests this may be the least consistently formalized of the three methods across the libraries studied, a pattern consistent with the absence of a documented security policy noted earlier in this study.

### **5.0 Conclusion and Recommendations**

The security of print and non-print materials is central to librarians' efforts to prevent unauthorized access to collections and to protect the resources on which teaching, learning, and research depend. This study examined information resources security management in public university libraries in Kano State using the House Security Management Model as an interpretive framework, and the findings indicate that the security problems these libraries face, unauthorized removal and physical damage, concealment and circumvention of physical controls, circulation-stage breaches, and identity and access-control breaches, are not attributable to the complete absence of any single security factor but to inconsistent application across the model's five factors: governance, operational processes, people awareness and training, physical and technological measures, and security culture. The libraries studied have adopted recognizable methods, electronic surveillance, personnel-based monitoring, and access control, yet the persistence of the issues identified suggests these methods are not yet operating as a coordinated system in the sense the model describes, where weakness in one factor, particularly governance and security culture, can undermine the protective value of strength in the others.

This points to a specific and addressable gap: the absence, noted by participants across the libraries studied, of a documented security policy formalizing the rules, procedures, and sanctions currently applied informally or inconsistently. Closing this governance gap would not replace the physical and technological measures already in place but would give them the consistent institutional backing the model identifies as necessary for their effectiveness.

## **5.1 Recommendations**

Based on the findings of this study, the following recommendations are made to university library management in Kano State:

1. Management should develop and formally adopt a comprehensive library security policy that stipulates rules, procedures, and sanctions for both library users and library staff, addressing the governance gap identified as the most consistently absent factor across the libraries studied.
2. Libraries should extend CCTV coverage to all units within the library, including entry and exit points, special collections, and areas where concealment behaviors such as hiding books in bags or clothing were reported, so that users are monitored from all angles rather than at isolated checkpoints.
3. Library management should formalize personnel-based monitoring into a defined operational schedule, specifying which staff are responsible for floor observation and circulation-desk monitoring at particular times, rather than relying on informal staff vigilance, to strengthen the operational-process factor identified in the findings.
4. Libraries should introduce or standardize identity verification procedures at entry points, including consistent use of identity cards and security personnel, to address the access-control breaches (impersonation and unauthorized access) reported by participants.
5. Management should institute regular staff training on security procedures and user monitoring, to build the people-awareness and security-culture factors that the findings suggest are the weakest link even where physical and technological measures are already present.
6. Libraries should review and strengthen circulation policies, including clearer sanctions for non-return of borrowed materials, to close the circulation-stage gap identified as distinct from physical-control breaches.

## **6.0 Limitations and Future Research Directions**

This study has several limitations that should be considered when interpreting its findings. First, the study was confined to four public university libraries in Kano State, with three librarians interviewed per institution; the findings therefore reflect the perspectives of personnel in these specific institutions and are not intended to be generalized to private or federal university libraries, or to public university libraries outside Kano State. Second, participants' accounts, particularly under the first research objective, were often brief single statements rather than extended narrative descriptions, which limited the depth of contextual detail available for some themes, notably the circulation-stage and identity-related breaches, where only one or two participants provided illustrative accounts. Third, the study relied solely on self-reported accounts from library personnel; no direct observation of library premises, incident records, or documentary evidence (such as existing security policies or theft logs) was used to corroborate participants' statements, which means the findings describe how personnel characterize security issues and methods rather than an independently verified record of security incidents or measures. Fourth, purposive sampling was used to select participants based on their circulation-related roles, which was appropriate for the study's objectives but means the perspectives of other library staff, such as those working exclusively in reference, technical services, or ICT units, were not captured. Finally, the cross-sectional design captured security issues and methods as they stood at a single point in time and cannot speak to how these issues or the libraries' responses to them have changed over time.

These limitations point to several directions for future research. Future studies could incorporate document analysis of existing (or absent) library security policies alongside interview data, to assess directly whether the governance gap identified in this study reflects a genuine absence of formal policy or an enforcement gap in policies that already exist. Comparative research across public, private, and federal university libraries in Kano State, or across university libraries

in other Nigerian states, could examine whether the pattern of uneven application across the House Security Management Model's five factors observed here holds in institutions with different funding levels and governance structures. Future research could also draw on a wider range of library staff roles, including reference, technical services, and ICT personnel, to determine whether security issues and methods are perceived differently outside the circulation function. Longitudinal research following a library's security practices before and after the adoption of a formal security policy could establish whether policy formalization produces the reduction in security breaches the present findings imply. Finally, future studies could combine interview data with incident-log analysis or direct observation of circulation and exit points, to test empirically whether the operational and cultural gaps identified through personnel accounts in this study correspond to observable patterns of security breaches.

## References

- Agboola, B., & Aduku, B. S. (2019). Managing security issues in Federal University Gashua Library, Yobe State, north east Nigeria [Conference presentation]. 1st International Conference on Personal Security and Community Policing, Alqalam University, Katsina, Nigeria.
- Basaka, A. A., Abdullahi, S., Dewa, A., & Barkindo, A. (2020). Security challenges and control measures in four academic libraries in North East Nigeria. *Journal of Science, Technology and Education*, 8(1), 100–108. <https://www.atbuftejoste.com>
- Chinwendu, N. A. (2019). Effect of theft and mutilation on the use of library collection in an academic library in Lagos State. *Library Philosophy and Practice*. <https://digitalcommons.unl.edu/libphilprac/2548>
- Elizabeth, E. E., & Ogunjimi, E. O. (2019). Overview of security measures in Nigerian university libraries. *Journal of Advances in Library and Information Science*, 8(1), 13–20. <https://jalis.in/pdf/8-1/Ekong.pdf>
- Gupta, P., & Madhusudhan, M. (2021). RFID technology as a potential electronic security system: An assessment from twenty-four academic libraries of India. *Journal of Knowledge & Communication Management*, 11(2), 87–115. <https://doi.org/10.5958/2277-7946.2021.00007.3>
- Igbinoia, M. O., & Ishola, B. C. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. *Digital Library Perspectives*, 39(3), 248–266. <https://doi.org/10.1108/DLP-11-2022-0089>
- Maidabino, A. A. (2016). Collection security management at university libraries: Assessment of its implementation status. *Journal of Library and Information Science*, 16(1), 15–33.
- Mindapa, A. (2022). Security problems of academic libraries in Nigeria. *Library Philosophy and Practice*. <https://scholarworks.sjsu.edu/libphilprac/7218>
- Ofori, K. S., Anyigba, H., Ampong, G. O. A., Omoregie, O. K., Nyamadi, M., & Fianu, E. (2022). Factors influencing information security policy compliance behaviour. In *Research anthology on business aspects of cybersecurity* (pp. 213–232). IGI Global. <https://doi.org/10.4018/978-1-6684-3698-1.ch010>
- Oladapo, Y. A., & Yusuf, F. O. (2022). Physical security measures in Nigerian polytechnic libraries: Challenges and prospects. *Library Management*, 43(5), 321–335.
- Olajide, O. (2017). Theft and mutilation challenges and management in academic libraries: A case study of Federal University Oye-Ekiti, Nigeria. *Journal of Applied Information Science and Technology*, 10(1). [https://www.jaistonline.org/10vol1/JAIST\\_PAPER\\_10\\_Theft\\_and\\_Mutilation\\_Challenges\\_recent.pdf](https://www.jaistonline.org/10vol1/JAIST_PAPER_10_Theft_and_Mutilation_Challenges_recent.pdf)
- Omoike, A., & Alabi, R. (2020). Theft, mutilation, and abuse of library and information materials by undergraduates of the University of Ibadan, Nigeria. *Information Impact: Journal of Information and Knowledge Management*, 11(2), 1–12. <https://doi.org/10.4314/ijikm.v11i2.1>
- Osayande, O. (2019). *Use of electronic security systems in academic libraries: Experiences of selected universities in South West Nigeria* [Doctoral dissertation, University of KwaZulu-Natal].