EVALUATION OF SECURITY MEASURES FOR SUSTAINABLE INFORMATION SYSTEMS IN PUBLIC UNIVERSITY LIBRARIES IN NIGERIA

BY

Mohammed Safiya Garba[1] Hussaini Musa[2] Rhoda Wusa Goshie[3]
Federal University of Technology Minna [123]
Correspondence Email: safiamah2278@gmail.com

Abstract

The security of information systems in public university libraries remains a critical concern in the digital era, where both physical and electronic resources are increasingly vulnerable to misuse, theft, and cyber threats. This opinion paper argues that effective security measures are not merely technical add-ons but core components of sustainable library management. While many libraries in developing contexts focus on acquiring ICT infrastructure, insufficient attention is paid to robust security protocols such as access control, authentication systems, data encryption, surveillance, and disaster recovery plans. The absence of these measures often results in breaches that compromise not only the integrity of library collections but also user trust and institutional credibility. This paper contends that libraries should move beyond reactive security practices toward proactive, policy-driven frameworks that integrate technological safeguards with user education. Furthermore, the sustainability of these measures depends on regular staff training and adequate funding support from university management. Strengthening security measures is, therefore, not an optional administrative function but a strategic imperative for ensuring the long-term viability and relevance of public university libraries in an increasingly digital knowledge environment.

Keywords: Security Measures, Information Systems, Public University Libraries, ICT Infrastructure, Library Management, Sustainability, Digital Resources.

Introduction

In the digital era, information systems serve as the backbone of academic librariesespecially public university librariesby enabling streamlined access to digital collections, interlibrary loans, and institutional repositories. Yet as these systems grow more sophisticated, they also become targets for cyberthreats and data breaches. Okike and Adetoro (2019) observed widespread malware attacks targeting OPAC and operating systems in university libraries in southwest Nigeria, highlighting that while some technical defenses like firewalls exist, effective access control systems are often lacking . Moreover, Owate (2022) underscored how poor information security management can undermine sustainable learning among library professionals, calling attention to the human and organizational dimensions of security . These findings collectively emphasize that the sustainability of information systems hinges not just on technology, but on organizational readiness and human-centered measures.

Beyond technical safeguards, developing facilitating conditionslike adequate ICT skills, awareness campaigns, and policy supportproves vital. Esse and Haliso (2024), investigating institutional repository sustainability in Nigerian public universities, found that current awareness and ICT competency significantly influence the continuation of digital services . Additionally, Obim and Akpokurerie (2023) revealed low levels of cybersecurity awareness among librarians in southeastern Nigeria, paired with insufficient training and policy frameworks, which undermines effective information storage . Without attention to these enabling factors, libraries may struggle to build secure systems that endure over time.

Information systems in university libraries refer to the integrated set of technologies, people, and processes used to manage and deliver information resources to academic communities. They encompass both traditional library automation toolssuch as Online Public Access Catalogues (OPACs), databases, and integrated library management systemsas well as newer digital infrastructures like institutional repositories, RFID-based tracking systems, and electronic security devices. As Ismail and Zainab (2017) noted, information systems are central to library operations, but their effectiveness depends on both technological robustness and organizational readiness. In the context of public university libraries in Nigeria, these systems not only facilitate research and learning but also represent valuable institutional assets that must be safeguarded.Samson etal (2015) stated that the technology behind information systems in today's world has been embedded in nearly every aspect of our lives. Thus, the idea of securing our information systems and/or computer networks has become very paramount. Owing to the significance of computer networks in transporting the information and knowledge generated by the increased diversity and sophistication of computational machinery, it would be very imperative to engage the services of network security professionals to manage the resources that are passed through the various terminals (end points) of the these network, so as to achieve a maximum reliability of the information passed, making sure that this is achieved without creating a discrepancy between the security and usability of such network.

Security measures in libraries, on the other hand, are the strategies, technologies, and policies designed to protect information systems from threats such as theft, vandalism, unauthorized access, and cyberattacks. Scholars like Osayande (2013) and Okike and Adetoro (2019) have shown that while some libraries adopt electronic security systems such as CCTV, smart cards, and firewalls, gaps remain in access control, monitoring, and staff compliance. Security measures are generally categorized into administrative controls (policies, regulations, audits), technical controls (firewalls, passwords, RFID, authentication protocols), physical controls (locks, alarms, surveillance), and human factors (training, awareness, compliance). The absence of a comprehensive mix of these dimensions leaves libraries vulnerable and undermines the reliability of their systems.

Sustainability, in the context of information systems, refers to the capacity of libraries to ensure the continuity, resilience, and long-term reliability of digital and physical information services despite evolving threats. Esse and Haliso (2024) stressed that sustainability in library systems is tied not only to infrastructure but also to ongoing awareness creation, ICT skill development, and institutional support. Similarly, Owate (2022) argued that information security management is critical for sustaining professional learning and service delivery in libraries. This means that sustainability is not achieved once and for all but requires continuous investment in infrastructure, policies, and staff attitudes. In this paper, sustainability is understood as the ability of public university libraries to provide secure, reliable, and uninterrupted access to information resources through robust and holistic security measures.

The Centrality of Security Measures

Security measures are the backbone of sustainable information systems in public university libraries. Without well-defined security frameworks, even the most advanced systems remain fragile and prone to collapse. As Singh and Kumar (2021) observe, the growing reliance on digital library services has expanded the threat landscape, making security protocols indispensable. In Nigeria, public university libraries face unique risks such as inadequate surveillance systems, poor cybersecurity defenses, and theft of print and electronic resources. Strengthening these measures requires a layered approachphysical, digital, and administrativeso that no single failure exposes the entire system. This aligns with the argument of Adebayo and Omotayo (2020) that libraries must treat security as a strategic priority, not an afterthought.

The Role of Staff Attitude and Institutional Culture

Even the most sophisticated technologies can fail if library staff and users do not uphold security protocols. Human behavior is often the weakest link in any security system. Staff negligence, deliberate sabotage, or lack of training can render security technologies ineffective. As Fatoki (2022) emphasized, organizational culture and staff attitudes strongly influence how security measures are implemented and maintained. A sustainable approach therefore requires fostering a culture of compliance, accountability, and awareness. Training programs, periodic sensitization workshops, and clearly defined sanctions for breaches are essential for creating a proactive workforce. This is particularly important in Nigeria, where many libraries still struggle with low staff-to-technology alignment (Okike & Adetoro, 2019).

Integrating ICT Infrastructure for Long-term Sustainability

A sustainable information system cannot exist without reliable ICT infrastructure. Power supply, internet connectivity, digital storage, and system interoperability are critical enablers of library security. In their study, Ese and Haliso (2024) found that ICT skill development among staff directly correlates with the effectiveness of security systems. In many Nigerian public university libraries, however, ICT facilities are outdated or poorly maintained, making them ill-equipped to handle emerging security challenges. Investment in modern ICT infrastructuresuch as cloud-based storage, automated access systems, Radio Frequency Identification Technology (RFID) and AI-driven surveillancecan significantly improve resilience. This requires not only financial resources but also strong partnerships with government, donors, and technology providers. Without this integration, sustainability will remain an elusive goal.

Challenges in Strengthening Security Measures

Despite the recognition of security as a core requirement, libraries still grapple with systemic challenges. Chief among them is inadequate funding, which prevents the acquisition of modern technologies and recruitment of skilled personnel. In addition, irregular power supply in Nigeria hinders the use of ICT-based security systems. Another challenge lies in policy gapsmany libraries lack clear, documented security policies, making enforcement inconsistent. As observed by Nkiko (2020), without formal security policies, libraries are forced into reactive measures rather than proactive planning. These challenges, if unaddressed, undermine any effort to make information systems sustainable.

Challenges in Strengthening Security Measures in Public University Libraries

1. Inadequate Funding

Most public university libraries operate on limited budgets, making it difficult to invest in modern security technologies (RFID, CCTV, access control). Funds are often prioritized for collections and academic services rather than security.

2. Poor ICT Infrastructure

Weak internet connectivity, outdated systems, or lack of reliable power supply hinder the implementation of digital security measures. Without stable infrastructure, technologies like RFID and surveillance systems cannot function effectively.

3. Insufficient Staff Training

Many librarians and staff members lack the technical skills to manage and operate advanced security systems. This leads to underutilization of tools, weak enforcement of policies, and loopholes in security management.

4. User Misconduct and Non-compliance

Students and even some staff may engage in theft, mutilation of books, or misuse of digital resources. Enforcing compliance is challenging due to high user populations and limited monitoring personnel.

5. Resistance to Change and Policy Gaps

Libraries may lack clear, updated security policies, and staff/users may resist new rules or technologies. Institutional bureaucracy also slows down adoption of stronger security measures.

ISSN: 3027-110X

Best Practices for Enhancing Security

Several libraries globally and within Africa have successfully implemented sustainable security models that can inspire Nigerian institutions. For example, the use of RFID technology in South African university libraries has significantly reduced book theft and enhanced resource tracking (Mabunda & Fourie, 2021). Similarly, some Nigerian universities have started adopting biometric authentication for user access, improving accountability. Other best practices include constant staff retraining, collaborations with ICT experts, adoption of open-source security software, and community policing approaches where students and staff share responsibility for safeguarding resources. These practices show that innovation, adaptability, and inclusivity are key to long-term sustainability.

Best Practices for Enhancing Security

1. Adoption of RFID and Digital Tracking Systems
RFID improves efficiency in tracking, circulation, and theft prevention. Research shows that libraries using RFID experience reduced resource losses and better inventory control.
2. Regular Staff Training and Capacity Building
Continuous training ensures staff can operate, monitor, and troubleshoot security systems. Well-trained staff are also better at detecting suspicious behavior and enforcing policies.
3. Integration of ICT Infrastructure with Security Systems
Linking library systems (OPAC, digital repositories) with security tools (firewalls, authentication, surveillance) creates a holistic protection framework. Research indicates ICT-backed security yields better results than isolated measures.
4. User Awareness and Orientation Programs
Educating users about security policies, responsible use of resources, and consequences of misconduct reduces theft, vandalism, and digital misuse. Studies show compliance improves when users are sensitized.
5. Regular Security Audits and Policy Updates
Periodic checks on both physical and digital systems help identify vulnerabilities. Updating policies in line with technological and institutional changes ensures security remains effective.

The Way Forward

To ensure sustainable information systems in public university libraries, a multi-stakeholder strategy is necessary. Government agencies must prioritize funding for library security infrastructure as part of national educational development. University management should develop enforceable security policies and establish dedicated security committees for libraries. Librarians must embrace continuous professional development, while users should be sensitized to view security as a shared responsibility. Furthermore, collaboration with international organizations can bring in expertise, funding, and technology transfer. Ultimately, sustainability depends on viewing security not just as a technical challenge, but as an institutional culture and collective commitment.

Conclusion

The sustainability of information systems in public university libraries depends heavily on the strength of their security measures and the attitudes of staff who manage them. A secure library environment is not achieved through technology alone but through the synergy of policies, infrastructure, and human commitment. As the discussion has shown, robust ICT infrastructure, continuous staff training, and positive organizational culture are critical in overcoming security challenges. Without these, public university libraries remain vulnerable to theft, data breaches, and operational inefficiencies that compromise their mission of supporting teaching, learning, and research.

Recommendations

1. Policy Development and Enforcement: University libraries should establish clear, comprehensive security policies that define staff and user responsibilities, sanctions for violations, and protocols for managing risks.

2. Investment in ICT Infrastructure: Governments, donor agencies, and university management should prioritize the provision of reliable ICT infrastructure such as RFID, biometric access, CCTV, and cloud storage systems.
3. Staff Training and Awareness: Regular workshops and capacity-building programs should be conducted to improve staff competence and foster a security-conscious organizational culture.
4. Collaborative Security Models: Libraries should adopt participatory approaches that involve staff, students, and community stakeholders in safeguarding resources.
5. Sustainable Funding Mechanisms: University management should allocate dedicated funds for security and explore external funding opportunities through partnerships with NGOs and international agencies.
6. Monitoring and Evaluation: Security measures should be continuously assessed and improved through audits, feedback systems, and benchmarking against best practices in other universities.

References

Akor, P. U., Nongo, S. I., & Idachaba, I. A. (2023). Emerging technologies and the future of library security in Nigeria. South African Journal of Science, 119(11/12), 16671. https://unisapressjournals.co.za/index.php/sajs/article/view/16671

Akpan, A. G., Udofot, C. O., Onyeneho, B. U., & Nwagidi, U. F. (2023, October). Harnessing cybersecurity paradigms for library services. In Proceedings of the 4th National Conference of the Nigerian Library Association, Nasarawa State Chapter (pp. 133–145). Nigerian Library Association.https://www.researchgate.net/publication/374808030_Harnessing_Cybersecurity_Paradigms_for_Library_Services

Badamasi, S., & Utulu, S. C. A. (2021). A framework for managing cybersecurity in Nigerian universities. arXiv Preprint arXiv:2108.09754. https://arxiv.org/abs/2108.09754

Choobineh, J., Kaya, B., & Yildiz, S. (2024). Impact of information security awareness on information security compliance of academic library staff in Türkiye. Journal of Academic Librarianship, 50(4), 102794. https://doi.org/10.1016/j.acalib.2024.102794

Echem, M. E., & Okwu, E. (2023). Library security and sustainable service delivery in Donald Ekong Library, University of Port Harcourt. Communicate: Journal of Library and Information Science, 25(1), 89–101. https://www.cjolis.org/index.php/cjolis/article/view/26

Esse, U. C., & Haliso, Y. (2024). Institutional repository sustainability in Nigerian public universities: The roles of current awareness and ICT skills. Digital Library Perspectives, 40(2), 137–152. https://doi.org/10.1108/DLP-05-2023-0035

Ismail, R., & Zainab, A. N. (2017). Information systems security in special and public libraries: An assessment of status. Malaysian Journal of Library and Information Science, 16(2), 45–62. https://mjlis.um.edu.my/article/view/6697

Obim, E., & Akpokurerie, R. (2023). Awareness of cybersecurity and its impact on information storage in the university libraries in South East Nigeria. Nigerian Libraries, 56(1), 23–38. https://www.researchgate.net/publication/377308149_AWARENESS_OF_CYBERSECURITY_AND_ITS_IMPA

CT_ON_INFORMATION_STORAGE_IN_THE_UNIVERSITY_LIBRARIES_IN_SOUTH_EAST_NIGERIA

Okike, B. O. I., & Adetoro, N. (2019). Are there threats to information system security? A focus on university libraries in South-West, Nigeria. Gateway Information Journal, 20(1), 1–15. https://www.gatewayinfojournal.org/index.php/gij/article/view/26

Osayande, O. (2013). Electronic security systems in academic libraries: A case study of three university libraries in South-West Nigeria. Chinese Librarianship: An International Electronic Journal, 32, 1–14. https://researchspace.ukzn.ac.za/items/b34a4504-ce82-4312-912a-db8b68e0f9e4

Owate, C. (2022). Information security management for sustainable learning among library and information science professionals in Nigeria. Library Philosophy and Practice (e-journal), Article 8522. https://acspublisher.com/journals/index.php/lp/article/view/8522

Samson, Grace and Usman, Mistura M. (2015) Securing an Information Systems from Threats: A Critical Review. International Journal of Computer Applications Technology and Research, 4 (6). pp. 425-434. ISSN 2319-8656

Umar, L. (2024). Electronic security management in libraries and information centres: Issues and challenges. In Proceedings of the 5th International Library and Information Science Conference (LISACON) (pp. 212–224). ResearchGate. https://www.researchgate.net/publication/385954205_Electronic_Security_Management_in_Libraries_and_Information_Centres_Issues_and_Challenges