International Journal of Information Resource Management (IJIRM)
Volume 3, Number 4 (October, 2026)
E- ISSN: 1118-7786

CYBER-SECURITY PRACTICES AND DATA PRIVACY PROTECTION AMONG UNIVERSITY LIBRARY STAFF IN RIVERS STATE, NIGERIA

Amaechi Kingsley Okere,

Department of Library and Information Science, Faculty of Education, Rivers State University, Nkpolu-Oroworukwu, Port-Harcourt

Innocent Iwezor Ordu Ph.D

Department of Library and Information Science, Faculty of Education, Rivers State University, Nkpolu-Oroworukwu, Port-Harcourt

and

John Gibson Ogonu Ph.D

Department of Library and Information Science, Faculty of Education, Rivers State University, Nkpolu-Oroworukwu, Port-Harcourt

Abstract

This study examined the relationship between selected cyber-security practices and data privacy protection among library staff in public universities in Rivers State, Nigeria. Three research questions and corresponding hypotheses guided the study. A correlational research design was adopted. The population comprised all 39 professional and para-professional library staff from three public universities: Rivers State University (11), University of Port Harcourt (18), and Ignatius Ajuru University of Education (10). A census approach was used because of the manageable population size. Data were collected with a structured questionnaire titled the Cyber-Security Strategies and Data-Privacy Practices Questionnaire (CSSDPPQ). The instrument yielded an overall Cronbach's alpha reliability coefficient of 0.79. Data were analysed using the Pearson Product Moment Correlation statistic at the 0.05 level of significance. The findings revealed moderate positive and statistically significant relationships between password management ($r = 0.653$, $p < 0.05$), data encryption ($r = 0.634$, $p < 0.05$), regular software updates ($r = 0.670$, $p < 0.05$) and effective data privacy protection practices among the library staff. All three null hypotheses were rejected. The study concludes that stronger adherence to password management protocols, data encryption, and regular software updates is associated with higher levels of

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

self-reported data privacy protection. It is recommended that university libraries enforce mandatory password management policies, invest in robust encryption technologies, and institutionalize regular automated software updates across library systems. The correlational nature of the design and the modest sample size constitute important limitations that should be considered when interpreting the results.

Keywords: Cyber-security practices, data privacy protection, password management, data encryption, software updates, university libraries, library staff, Rivers State

Introduction

Cyber-security is a vital component of information management in contemporary organizations. It encompasses the strategies, technologies, and administrative policies designed to protect networks, systems, and data from unauthorized access, damage, or misuse (Fasasi & Akinyemi, 2023). In higher education institutions, cyber-security has become indispensable because of the large volumes of sensitive data handled daily, including student and staff personal information, research outputs, examination records, and institutional intellectual property. Effective cyber-security helps ensure the confidentiality, integrity, and availability of information systems through proactive technical and administrative measures (Tella & Oladokun, 2024).

University libraries operate within increasingly digital environments that include online catalogue, electronic databases, institutional repositories, and cloud-based systems. While digitization enhances access and efficiency, it simultaneously exposes libraries to cyber threats such as hacking, ransom ware, phishing, malware, and insider attacks (Ajuwon & Eze, 2024). Because library systems are often interconnected with broader university networks, a single breach can compromise academic, administrative, and

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

financial systems (Ibrahim & Odu, 2024). Sustaining digital library operations therefore requires robust and consistently implemented cyber-security practices.

Closely linked to cyber-security is data privacy, which refers to the lawful and ethical handling of personal and institutional information. Data privacy ensures that data are collected, stored, processed, and shared in accordance with principles of confidentiality, consent, and purpose limitation (Nigeria Data Protection Act, 2023). While cyber-security primarily secures technological infrastructure, data privacy governs behavioural and policy frameworks. The two are interdependent: effective data privacy depends on strong cyber-security measures (Ademola & Ogundele, 2023).

Core cyber-security practices password management policies, data encryption, and regular software updates directly support data privacy protection. Effective password policies promote strong and unique credentials and reduce unauthorized access (Akinwale, 2023). Data encryption renders sensitive information unreadable to unauthorized users, while regular software updates and patch management close vulnerabilities that attackers may exploit. However, weak policy enforcement, inadequate ICT funding, limited staff awareness, and uneven compliance with the Nigeria Data Protection Act continue to challenge effective implementation in Nigerian universities (Fasasi & Akinyemi, 2023; Nigeria Data Protection Commission, 2023). Given the central role of university libraries in academic ecosystems, examining how password management, data encryption, and regular software updates relate to data privacy protection among library staff in Rivers State universities is both timely and necessary. Such an examination can provide empirical

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

evidence to strengthen cyber-security practices, improve regulatory compliance, and enhance trust in digital library services.

Cyber-security is a critical component of modern information management, particularly in environments that depend heavily on digital technologies such as university libraries. While some authors distinguish cyber security from information security (Solms & Niekerk, 2013; Analytics India, 2020), both concepts converge on the protection of systems, networks, and data from digital attacks that may result in unauthorized access, destruction of information, or disruption of services (Raghavaiah & Srikanth, 2024). In academic libraries, the need for cyber-security has grown because these institutions manage sensitive information such as research data, digital collections, and personal records of users (Lee, 2022). The presence of diverse users—students, staff, and researchers increases the difficulty of securing systems and exposes libraries to threats such as hacking, malware, and ransom ware. Academic libraries have an ethical obligation to protect the privacy of their users and to ensure that personal information is not misused or compromised. Cyber-security therefore helps ensure that digital library systems operate securely while protecting the confidentiality and integrity of user information.

Effective cyber-security requires not only technological solutions but also competent personnel and sound institutional practices. Library staff must possess adequate cyber-security awareness and skills to implement protective measures and respond to incidents. This includes adopting secure password practices, maintaining updated software systems, and ensuring proper handling of sensitive information.

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Ultimately, cyber-security serves as a foundation for protecting digital library systems and supporting the secure delivery of academic library services.

Data privacy in academic libraries refers to the principles, policies, practices, and technical safeguards that govern the collection, storage, processing, and sharing of personal and institutional information. Its primary aims are to protect the privacy rights of users and to maintain institutional integrity. It encompasses both traditional confidentiality obligations (for example, protecting circulation records and reference queries) and modern privacy concerns associated with digital systems, including authentication logs, institutional repositories, learning analytics, and third-party service platforms (Hess, LaPorte-Fiori & Engwall, 2015).

Academic libraries face several privacy risks arising from the increasing use of digital technologies and third-party information systems. Technical risks include the generation of detailed user activity records that could enable profiling. Organizational risks arise from limited staff awareness, inadequate privacy policies, and poor data retention practices. Contractual risks emerge when libraries rely on third-party vendors who process or store user data on behalf of the institution (Singh & Singh Brar, 2024).

To address these challenges, academic libraries need clear privacy policies, data minimization practices, retention and disposal schedules, technical safeguards such as encryption and access controls, and ongoing staff training (Briney, 2019). Emerging technologies such as research data repositories, learning analytics, and artificial intelligence systems introduce additional privacy challenges that require careful

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

governance (Dube, 2025). Effective data privacy practices enable academic libraries to protect sensitive information, maintain user trust, comply with regulatory requirements, and support responsible information management.

Password management policies, data encryption, and regular software updates constitute core technical and administrative controls that support effective data privacy protection. Password management policies establish rules governing the creation, storage, and use of credentials. By enforcing strong and unique passphrases and discouraging weak authentication practices, libraries can reduce the risk of unauthorized access and credential compromise (NIST, 2017; Grassi et al., 2017). The integration of multi-factor authentication further strengthens protection against phishing and account takeover incidents.

Data encryption transforms readable information into cipher text accessible only to authorized users. Encryption at rest protects stored databases and backups, while encryption in transit secures data transmitted across networks (Dierks & Rescorla, 2018; NIST, 2018). Regular software updates and structured patch management reduce vulnerabilities that attackers commonly exploit. Timely updates correct security flaws and reinforce authentication and encryption modules (NIST, 2013; ENISA, 2018). Collectively, these practices provide a layered defense that helps library staff safeguard digital assets and protect user information.

Statement of the Problem

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

The rapid digitization of university library services in Rivers State has increased dependence on electronic databases, institutional repositories, and networked information systems. This dependence has exposed libraries to significant cyber-security risks, including unauthorized access, data breaches, and misuse of sensitive information. Library staff, as primary operators and custodians of these digital systems, is directly responsible for implementing cyber-security measures that protect personal and institutional data. However, the extent to which key cyber-security practices password management policies, data encryption, and regular software updates are associated with effective data privacy protection within university libraries remains unclear. Weak or inconsistent application of these practices may create vulnerabilities that compromise data privacy, system integrity, and the confidentiality of user information. Despite the existence of regulatory frameworks such as the Nigeria Data Protection Regulation (NDPR) and the Nigeria Data Protection Act 2023, concerns persist that many university libraries lack adequately enforced cyber-security policies, sufficient technical safeguards, and structured implementation of data protection measures.

Limited technical capacity, inadequate awareness, and poor compliance with established cyber-security protocols may weaken the ability of library staff to protect digital assets effectively. Consequently, there is a need to empirically examine the relationships between these cyber-security practices and effective data privacy protection among university library staff in Rivers State. Addressing this gap is essential for

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

strengthening information security, supporting regulatory compliance, and promoting secure and sustainable digital library operations.

Research Questions

The following research questions guided the study:

1. To what extent does password management relate to effective data privacy protection practices among library staff of Rivers State universities?

2. To what extent does data encryption relate to effective data privacy protection practices among library staff of Rivers State universities?

3. To what extent do regular software updates relate to effective data privacy protection practices among library staff of Rivers State universities?

Hypotheses

The following null hypotheses were tested at the 0.05 level of significance:

H_{01}: Password management does not significantly relate to effective data privacy protection practices among library staff of Rivers State universities.

H_{02}: Data encryption does not significantly relate to effective data privacy protection practices among library staff of Rivers State universities.

H_{03}: Regular software updates do not significantly relate to effective data privacy protection practices among library staff of Rivers State universities.

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Methodology

This study adopted a correlational research design. The population comprised all 39 professional and para-professional library staff in the three public universities in Rivers State: Rivers State University (11), University of Port Harcourt (18), and Ignatius Ajuru University of Education (10). A census sampling approach was used because of the manageable size of the population. Data were collected using a structured questionnaire titled the Cyber-Security Strategies and Data-Privacy Practices Questionnaire (CSSDPPQ). Section A captured demographic information, while Section B measured the study variables—password management, data encryption, regular software updates, and data privacy protection practices—using a four-point Likert scale (Strongly Agree, Agree, Disagree, Strongly Disagree).

Content validity was established through review by two experts in Library and Information Science at Rivers State University; their recommendations were incorporated. Reliability was assessed through a pilot test involving 20 library staff from a university outside the study area. The overall Cronbach's alpha coefficient obtained was 0.79. Subscale reliabilities were not separately reported in the original analysis.

The copies of the questionnaire were administered directly by the researcher with the assistance of two trained research aides after official permission had been obtained from library management. Data were analysed using the Pearson Product Moment Correlation coefficient to answer the research questions and test the hypotheses at the 0.05 level of significance.

Results and Discussion

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Research Question 1 and Hypothesis One

To what extent does password management relate to effective data privacy protection practices among library staff of Rivers State universities?

H_{01}: Password management does not significantly relate to effective data privacy protection practices among library staff of Rivers State universities.

Table 1: PPMC Summary on the relationship between password management and effective data-privacy protection practices among library staff of Rivers State Universities

		Password Management	Data-Privacy Protection
Password Management	Pearson Correlation	1	.653**
	Sig. (2-tailed)		.000
	N	39	39
Data-Privacy Protection	Pearson Correlation	.653**	1
	Sig. (2-tailed)	.000	
	N	39	39

**.Correlation is significant at the 0.05 level (2-tailed).

Table 1 shows a Pearson correlation coefficient of r = 0.653 between password management and effective data privacy protection practices. This indicates a moderate positive relationship. The relationship is statistically significant (p = .000 < .05). Consequently, the null hypothesis is rejected.

The finding suggests that as self-reported password management practices improve, self-reported data privacy protection also tends to improve. Adherence to secure password protocols—creating strong passwords, maintaining confidentiality of login credentials, and following institutional guidelines—appears to be associated with better protection of

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

sensitive information within library systems. This result is consistent with earlier observations that weak password practices increase system vulnerability, while strong password management supports the confidentiality and integrity of institutional data (Lee, 2022; Akinwale, 2023).

Research Question 2 and Hypothesis Two

To what extent does data encryption relate to effective data privacy protection practices among library staff of Rivers State universities?

H_{02}: Data encryption does not significantly relate to effective data privacy protection practices among library staff of Rivers State universities.

Table 2: PPMC Summary on the relationship between data encryption and effective data-privacy protection practices among library staff of Rivers State Universities

		Data Encryption	Data-Privacy Protection
Data Encryption	Pearson Correlation	1	.634**
	Sig. (2-tailed)		.000
	N	39	39
Data-Privacy Protection	Pearson Correlation	.634**	1
	Sig. (2-tailed)	.000	
	N	39	39

**.Correlation is significant at the 0.05 level (2-tailed).

Table 2 shows a Pearson correlation coefficient of r = 0.634 between data encryption and effective data privacy protection practices. This indicates a moderate positive relationship that is statistically significant (p = .000 < .05). The null hypothesis is therefore rejected.

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

The result indicates that greater use of encryption is associated with higher levels of self-reported data privacy protection. Encryption serves as a technical safeguard that helps protect the confidentiality of sensitive records during storage and transmission. This finding aligns with the established view that encryption is one of the most effective mechanisms for preventing unauthorised access to data (Stallings, 2017) and supports compliance with data protection requirements (NITDA, 2019).

Research Question 3 and Hypothesis Three

To what extent do regular software updates relate to effective data privacy protection practices among library staff of Rivers State universities?

H_{03}: Regular software updates do not significantly relate to effective data privacy protection practices among library staff of Rivers State universities.

Table 3: PPMC Summary on the relationship between regular software updates and effective data-privacy protection practices among library staff of Rivers State Universities

		Regular Software Updates	Data-Privacy Protection
Regular Software Updates	Pearson Correlation	1	.670**
	Sig. (2-tailed)		.000
	N	39	39
Data-Privacy Protection	Pearson Correlation	.670**	1
	Sig. (2-tailed)	.000	
	N	39	39

**.Correlation is significant at the 0.05 level (2-tailed).

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Table 3 shows a Pearson correlation coefficient of r = 0.670 between regular software updates and effective data privacy protection practices. This is a moderate positive relationship that is statistically significant (p = .000 < .05). The null hypothesis is rejected.

The finding indicates that consistent updating of software systems is associated with improved self-reported data privacy protection. Regular updates help fix security vulnerabilities and improve the resilience of information systems against cyber threats. This result is consistent with literature emphasising that outdated software is highly vulnerable to attack, while timely updates provide essential security patches (Kizza, 2017; NIST, 2018).

Limitations of the Study

Several limitations should be noted when interpreting the findings. First, the sample size of 39, although comprising the entire accessible population of professional and para-professional library staff in the three institutions, is modest. Correlation coefficients derived from small samples can be less stable, and statistical power is limited. Second, the study relied exclusively on self-reported data. Responses on security practices may be influenced by social-desirability bias. Third, only bivariate correlations were examined; the unique contribution of each practice after controlling for other variables was not assessed. Fourth, the study was restricted to three public universities in one Nigerian state; findings may not generalise to private universities or other geopolitical zones. Finally, subscale reliability coefficients for the individual constructs were not separately reported.

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Recommendations

Based on the findings, the following recommendations are made:

1. University management should establish and enforce comprehensive password management policies that require strong, unique passwords and, where feasible, multi-factor authentication across all library systems.
2. Libraries should implement robust data encryption protocols for both data at rest and data in transit to safeguard sensitive patron and institutional information.
3. A systematic schedule for regular software updates and patch management should be institutionalised to protect library systems from known vulnerabilities and emerging cyber threats.

Conclusion

This study examined the relationships between three cyber-security practices—password management, data encryption, and regular software updates—and data privacy protection among library staff in public universities in Rivers State, Nigeria. The findings showed moderate positive and statistically significant associations between each of the three practices and self-reported data privacy protection.

The results suggest that when library staff report stronger adherence to these foundational security practices, they also tend to report higher levels of data privacy protection. Technology alone is insufficient; the daily choices of library staff—whether to

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

use strong passwords, apply encryption, or install updates—play an important role in the security of institutional and user information. The moderate strength of the relationships also indicates room for improvement through clearer policies, regular training, and systems that make secure behaviour easier to adopt.

Protecting data privacy in academic libraries is both a technical and a human responsibility. As digital transformation continues across Nigerian universities, sustained attention to these cyber-security practices will remain essential for safeguarding institutional data and maintaining user trust.

References

Ademola, S. O., & Ogundele, T. A. (2023). Cybersecurity and data privacy compliance in Nigerian higher institutions: Challenges and implications for information management. Journal of Information Policy and Governance, 8(2), 65–79.

Ajie, I. (2019). A review of trends and issues of cybersecurity in academic libraries. Library Philosophy and Practice (e-journal), 2523.

Ajuwon, A., & Eze, C. J. (2024). Cyber threats and mitigation strategies in Nigerian academic libraries. Library Philosophy and Practice, 2024(7564), 1–15.

Akinwale, J. M. (2023). Password management and digital safety awareness among university staff in South-West Nigeria. African Journal of Information and Communication Technology, 19(1), 44–57.

Al-Shboul, M., & Al-Mansour, J. (2023). Cybersecurity challenges and database protection strategies in higher education institutions. Journal of Information Security and Applications, 73, 103482. https://doi.org/10.1016/j.jisa.2023.103482

Analytics India Magazine. (2020). Cybersecurity: Difference between cybersecurity & information security. https://analyticsindiamag.com/difference-between-cybersecurity-information-security/

Bhavsar, S., & Bhavsar, S. (2017). Cyber crimes and measures to prevent in libraries. Knowledge Librarian, 3(5), 38–47.

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Briney, K. A. (2019). Data management practices in academic library learning analytics: A critical review. Journal of Librarianship and Scholarly Communication, 7(1). https://doi.org/10.7710/2162-3309.2268

Dierks, T., & Rescorla, E. (2018). The transport layer security (TLS) protocol version 1.3 (RFC 8446). Internet Engineering Task Force. https://doi.org/10.17487/RFC8446

Dube, T. V. (2025). Research data management in academic libraries: Institutional repositories as a reservoir for research data. Library Management, 46(5), 319–331.

European Union Agency for Cybersecurity (ENISA). (2017). Good practices on the security of personal data processing.

Fasasi, R. A., & Akinyemi, B. T. (2023). Cybersecurity governance in Nigerian higher education institutions: Policy and practice gaps. Nigerian Journal of Educational Technology, 6(2), 112–128.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: Authentication and lifecycle management (NIST Special Publication 800-63B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B

Hernández-Rosales, J., & Figueroa, O. (2021). Protecting digital assets in academic libraries through enhanced cybersecurity governance. The Electronic Library, 39(6), 1002–1017. https://doi.org/10.1108/EL-02-2021-0041

Hess, A. N., LaPorte-Fiori, R., & Engwall, K. (2015). Preserving patron privacy in the 21st century academic library. The Journal of Academic Librarianship, 41(1), 105–114. https://doi.org/10.1016/j.acalib.2014.10.010

Ibrahim, U. A., & Odu, C. A. (2024). Digitization and information security in university libraries: A study of Nigerian institutions. Information Management Review, 12(1), 51–70.

Injac, O., & Sendelj, R. (2016). National security policy and strategy and cyber security risks. In M. Hadji-Janev & M. Bogdanoski (Eds.), Handbook of research on civil society and national security in the era of cyber warfare (pp. 22–48). IGI Global.

International Organization for Standardization/International Electrotechnical Commission. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

International Organization for Standardization/International Electrotechnical Commission. (2017). ISO/IEC 27002:2017 Information technology — Security techniques — Code of practice for information security controls.

Lee, S. (2022). The impact of cybersecurity threats on academic libraries. Journal of Library Technology, 39(4), 120–134.

National Information Technology Development Agency (NITDA). (2019). Nigeria data protection regulation (NDPR). Federal Republic of Nigeria.

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

National Institute of Standards and Technology. (2013). Security and privacy controls for federal information systems and organizations (NIST Special Publication 800-53).

National Institute of Standards and Technology. (2017). Digital identity guidelines (NIST Special Publication 800-63).

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity.

Nigeria Data Protection Act, 2023. Federal Republic of Nigeria Official Gazette. Nigeria Data Protection Commission.

Raghavaiah, P., & Srikanth, K. (2024). The importance of cybersecurity in academic libraries in modern age. Proceedings of the 12th International Library and Information Professionals Summit (ILIPS).

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125–128.

Singh, S., & Singh Brar, K. (2024). Academic libraries and their patrons' digital data privacy: A systematic literature review. College Libraries, 38(4).

Solms, R. v., & Niekerk, J. V. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson Education.

Sturges, P. (2022). Privacy, data protection and user rights in the digital library environment. IFLA Journal, 48(2), 225–240. https://doi.org/10.1177/03400352211029224

Tella, A., & Oladokun, O. S. (2024). Cybersecurity literacy and data-privacy awareness among library staff in Nigerian universities. Journal of Information Security Education, 14(3), 77–93.

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)