British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 123-136)
www.abjournals.org

DATA HANDLING STAGES AND INFORMATION SECURITY PRACTICE AMONG NON-ACADEMIC STAFF OF STATE-OWNED POLYTECHNICS, OYO STATE, NIGERIA

Tolulope Elizabeth Adenekan (Ph.D.)[1] and Ibrahim Sunday Oyekola[2].

[1]Department of Office and Information Management, Lead City University, Ibadan, Nigeria.
Email: tolu.adenekan@lcu.edu.ng

[2]Department of Office and Information Management, Lead City University, Ibadan, Nigeria.
Email: oyekolakanmi@gmail.com

Cite this article:

T. E., Adenekan, I. S., Oyekola (2026), Data Handling Stages and Information Security Practice among Non-Academic Staff of State-Owned Polytechnics, Oyo State, Nigeria. British Journal of Computer, Networking and Information Technology 9(1), 123-136. DOI: 10.52589/BJCNIT-WMFXRIE4

Manuscript History

Received: 20 Oct 2025

Accepted: 24 Nov 2025

Published: 19 Mar 2026

ABSTRACT: *Information security serves as the strategic effort to shield data from threats. This study investigated the influence of data handling stages and information security practices among Non-Academic staff of State–owned polytechnics, Oyo State, Nigeria. The study was guided by Traid CIA model and Record Continuum Model and used a descriptive survey design, for the population of 1109. The sample size for the study is 285 which was derived using Krejcie and Morgan sample size table and stratified sampling techniques was employed. Tools for data collection was a structured questionnaires which was administered across these three polytechnics (The Polytechnic, Ibadan; Adeseun Ogundoyin Polytechnic, Eruwa; The Oke-Ogun Polytechnic, Saki); after which 272 valid responses were analyzed using SPSS. Descriptive results showed a high level of information security practice, and a high implementation of data handling stages with a smaller significant contribution. The findings indicate that strong role and permission management substantially enhance the confidentiality, integrity, and availability of institutional records. In contrast, gaps in systematic classification, archiving, monitoring of system use, and control of unauthorized software weaken overall resilience. The study concludes that institutionalizing clear data-handling procedures, instituting regular training and periodic user-access reviews will substantially improve information security among registry staff.*

KEYWORDS: Information security practice; data handling stages; non-academic staff, state polytechnics.

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 123-136)

www.abjournals.org

INTRODUCTION

Information security refers to the strategies and actions taken to protect the privacy, accuracy, and accessibility of data. With the rapid adoption of digital innovations like cloud computing, artificial intelligence (AI), and the Internet of Things (IoT), the need to safeguard digital assets has grown more urgent than ever. While developed nations have long integrated information security into their organizational frameworks, many developing countries are now increasingly following suit. According to Nyame and Qin (2020) Information security is about defending digital systems and the information they hold from misuse, exposure, disruption, or alteration, preserving their confidentiality, integrity, and availability at all times. Organizational data must be carefully guarded to maintain its privacy, accuracy, and accessibility. In the opinion of Adenekan and Ologbosere (2021), depending on its nature, some information may demand protection on several fronts, highlighting the varied requirements involved in managing and securing data across different areas of an organization. The foundation of information security consists of the three properties, which are confidentiality, integrity and availability (Ameer, Benson and Sandhu, 2022). For the purpose of this study, information security refers to the ongoing effort to maintain the privacy, accuracy, and accessibility of data. Beyond these core principles, it may also encompass additional elements like authenticity, accountability, non-repudiation, and reliability. Sibai, Gemayel, Bou-Abdo and Demerjian (2019) opined that, the foundational pillars of information security, as outlined in the widely recognized CIA triad, are confidentiality, integrity, and availability. Confidentiality means information is disclosed to an authorized user within and outside the academic community, information integrity means information is not modified by an unauthorized user, and information availability means information is available when required to an authorized user.

A factor that could enhance the security of information and data among Non-Academic Staff in Oyo State-owned Polytechnics is how efficient they handle and manage information and data being guided by the policy and guidelines of the institutions. Data handling stages occupies a strategic position in the efficient and effective management of the Polytechnic system. In fact, according to Flynn (2001) it is central in the administration of institutions of learning because it documents the planning and implementation of appropriate courses of services, allowing proper monitoring of work. Data refer to raw information, regardless of form or medium, received and maintained by an institution, organization or individual in pursuance of its legal obligations or in the transaction of academic activities of any kind (Marshall, 2000). Data can be said to be any information or communication captured and retained in some reproducible media. Data in this case become the object, the document or medium, which carries the information. Data therefore, are information media created and valuable enough to be retained. Data could be in paper-based, that is to say that the information was captured on paper. However, the media for information carriage can also be in other forms like machine readable disks, graphics, images, diskettes, flash drives and pictorial media, be they photographic or/not (Yang, 2023).

Handling of data is therefore concerned with the creation, classification, scheduling and maintenance, and use of information among Non-Academic Staff as adopted from the records continuum model (Ahmadi, 2024). Data creation is the process of generating new data or information, either manually or automatically, through various methods such as collecting, recording or synthesizing. Data classification is the process of organizing data into categories or groups based on specific criteria such as sensitivity, type, of purpose, to facilitate

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

management, security. Data scheduling refers to the process of planning and automating the timing of data with related tasks such as collection, processing, or transfer. Data maintenance is the ongoing process of managing and updating data to ensure its accuracy, consistency and usability which includes tasks like cleaning data (removing duplicates or errors), updating records, archiving outdated data and ensuring data integrity and security. Use of information is the application of data, knowledge, or resources in scholarly and administrative activities; it involves accessing, analyzing, synthesizing and citing information from credible sources.

Information security is significant to maintaining the privacy and integrity of sensitive data, which helps safeguard both institutional and personal assets. Non-Academic Staff in Oyo State-owned polytechnics are involved in handling administrative tasks. Preliminary investigations, close observation, and literature reviews have identified a growing risk of information security threats to these institutions, particularly with their duties. If solutions are not implemented, there will be increased cyberattacks, loss of confidential information, and disruption of academic activities. Data handling stages have therefore been identified as key factor influencing information security among Non-Academic Staff in these institutions. This study however, examines the influence of data handling stages on information security practices among Non-Academic Staff in Oyo State-owned polytechnics, Nigeria. The research questions are:

i. What is the level of information security practiced by Non-Academic Staff in Oyo State-owned Polytechnics, Nigeria?

ii. What are the data handling stages practiced by Non-Academic Staff in Oyo State-owned Polytechnics, Nigeria?

While the research hypothesis is: there will be no significant influence of data handling stages on information security among Non-Academic Staff in Oyo State-owned Polytechnics.

LITERATURE REVIEW

Information forms the backbone of contemporary society, functioning as refined data that carries significance and context. At its core, it represents knowledge, facts, insights, or viewpoints that can be shared and understood through various channels. Its true value lies in its power to guide decisions, spark innovation, and drive advancement across every field of human activity. Security involves a wide range of methods and guiding principles aimed at safeguarding valuable assets from damage, unauthorized use, or potential loss. Security as a concept has undergone major transformation over time, evolving to meet the demands of emerging threats brought on by technological progress. Information security is all about defending data and the systems that handle it from unauthorized access, misuse, leaks, disruptions, or tampering. Its goal is to preserve three essential qualities: confidentiality, limiting access to only those who are authorized; integrity, ensuring the data remains accurate and unchanged; and availability, keeping information accessible whenever it is needed. Information security enables organizations to tackle threats like cyberattacks and internal breaches, helping them maintain smooth operations and build trust[1].

Information security is understood as the effort to maintain the privacy, accuracy, and accessibility of an organization's data assets (Aladesanmi, Afolabi and Oyebisi, 2012).

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 123-136)
www.abjournals.org

According to Bakare, Adeniyi, Akpuokwe and Eneh (2024), information security refers to the safeguarding of data and digital systems against threats like unauthorized access, misuse, exposure, disruption, alteration, or destruction. Its purpose is to ensure that valuable information remains protected and trustworthy throughout its lifecycle. Information security is often viewed as a mindset, one that involves recognizing its significance, staying alert to its goals, risks, and potential threats, and actively seeking the knowledge needed to engage with it responsibly. Research carried out by Boopathi (2023), suggests that when employees lack awareness or understanding of security policies and best practices, it becomes a leading factor behind poor security behavior and the negative outcomes that follow. Ultimately, the quality of information security depends on how confidential data is handled, the accuracy and reliability of information, and its availability when needed (El Filali, Bourian and Chougdali, 2024).

The Triad CIA model serves as a foundational framework in information security, defining three core principles: confidentiality, integrity, and availability. Confidentiality ensures that sensitive information is accessible only to authorized individuals. Integrity focuses on maintaining the accuracy, consistency, and trustworthiness of data throughout its lifecycle. While availability ensures that information and critical systems remain accessible to authorized users whenever needed (El Sibai, Gemayel, Bou Abdo and Demerjian, 2019).

Data handling stages outlines the formal procedures that dictate how an organization manages its information assets. It covers the entire lifecycle of data, from its collection and storage to its processing and distribution, ensuring that each stage complies with legal, ethical, and operational standards. Such policies are essential for maintaining data integrity, protecting sensitive information, and promoting accountability across all departments (Barata, Bennett, Cain, and Routledge, 2001). Data handling stages offer a comprehensive framework for managing information throughout its lifecycle, covering collection, storage, processing, and sharing. Its primary goal is to ensure that data is treated securely and consistently, thereby minimizing risks such as unauthorized access, data breaches, or loss. Data handling stages define the principles and procedures organization follows to manage personal data responsibly. It acts as a strategic guide, helping institutions navigate the complex landscape of data protection regulations. While outlining how data should be collected, stored, processed, and shared, the policy ensures consistency, accountability, and compliance with legal standards.

Data handling stage formalizes this process by setting out the standards and procedures for managing any information captured in reproducible form that is necessary for academic and administrative operations. According to IRMT (2009), such a policy ensures that data is consistently controlled, securely maintained, and readily accessible for authorized use, thereby supporting institutional efficiency, compliance, and informed decision-making. Over time, data handling stages have evolved from a primarily paper-based function, focused on storing an organization's miscellaneous documents, into a comprehensive framework for managing defined categories of internal data across multiple formats and media. The adoption of sound data handling stages delivers numerous benefits to institutional management. Foremost among these is the creation and maintenance of accurate, reliable data, enabling institutions to meet legal and regulatory obligations for data protection. Additional advantages include ensuring the legal admissibility of institutional records, reducing the reliance on and costs associated with paper-based record systems, and establishing effective strategies for migrating data to newer generations of technology and systems. The transition from traditional records

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

management to an electronic environment in Africa is unlikely to succeed unless the underlying processes are designed and implemented in an efficient and effective manner. In many cases, African states have embraced information technology initiatives without adequately integrating sound data handling policies into their frameworks. This oversight undermines the sustainability and effectiveness of such projects.

The Record Continuum Model has proven useful for data management stages because it covers the full lifecycle of records. This includes key processes like data creation, classification, scheduling, and maintenance, along with the proper use of information. The model highlights an integrated and ongoing approach to managing records, making sure each stage supports both organizational needs and information governance goals.

METHODOLOGY

This study adopted a descriptive survey design, with the population of one thousand one hundred and nine (1109) Non-Academic Staff in Oyo States-owned Polytechnics, Nigeria. The sample size of the population is two hundred and eighty five (285). This sample size was derived using Krejcie and Morgan's (1970) sample size table. Primary data was collected through a structured questionnaire and analyzed using descriptive and inferential statistics for the hypothesis.

FINDINGS

The demographic information of Non-Academic Staff in Oyo State-owned polytechnics indicates a slight dominance of female staff (140, 51.5%) over their male counterparts (132, 48.5%). For the age distribution, the largest group of respondents fall within the 46 and above category, with 128 staff members representing 51.9% of the total population. This is followed by 48 staff (16.6%) aged between 31-35 years. Both the 20–25 years and 36–40 years categories recorded 24 staff each (7%), while 16 respondents (11.8%) were between 26–30 years. Those aged 41–45 comprised 32 staff (10.8%), showing that while the workforce is predominantly old, a fair proportion of young and more experienced staff are also represented.

Regarding educational qualifications, the largest group of staff possess Higher National Diplomas (HND), accounting for 124 respondents (45.6%). This is followed by 60 respondents (22.1%) with Bachelor's degrees. Staff with NCE/OND and those with M.Sc. degrees each numbered 44 (16.2%), while no respondent reported holding a Ph.D. This reflects that the workforce largely consists of mid-level qualification holders. In terms of work experience, a minority of the staff have relatively shorter years of service. Specifically, 4 respondents (1.5%) reported having 5–10 years of work experience, making this the minority group. Another 48 staff (17.6%) had 16–20 years of experience, while 40 staff (14.7%) had served for 11–15 years. A smaller proportion of 16 respondents (5.9%) had 21–25 years of experience, and the majority of respondents 164 (60.3%) had worked for 26–30 years, showing that long-serving staff are relatively more and have good experience.

Research Question One: What is the level of information security practice among Non-Academic Staff in Oyo State-owned Polytechnics?

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 123-136)

www.abjournals.org

Table 1: Level of information security practice among Non-Academic Staff in Oyo State-owned Polytechnics.

Information Security	VH	H	L	VL	x
Information Confidentiality					
Acceptance guidelines for new information security	(107) 39.3%	(143) 52.6%	(21) 7.7%	(1) 0.4%	3.31
Existence of a network operational guideline in your organization	(40) 14.7%	(184) 67.6%	(48) 17.6%	(0) 0.00%	2.97
Identification of information security features	(68) 25.0%	(144) 52.9%	(60) 22.9	(0) 0.0%	3.03
Protection of system documentation against unauthorized access	(84) 30.9%	(148) 54.4%	(40) 14.7%	(0) 0.00%	3.16
Establishment of information exchange policy in your organization	(60) 22.1%	(164) 60.3%	(48) 17.6%	(0) 0.00%	3.04
Average Mean for Information Confidentiality					**3.10**
Information Integrity	**VH**	**H**	**L**	**VL**	**Mean**
Separation of the development of operational facilities	(68) 25.0%	(164) 60.3%	(40) 14.7%	(0) 0.00%	3.10
Existence of a policy prohibiting the use of unauthorized software in your organization	(60) 22.1%	(160) 58.8%	(52) 19.1%	(0) 0.00%	3.03
Backup policy for information	(112) 41.2%	(124) 45.6%	(36) 13.2%	(0) 0.00%	3.28
Policy to protect the electronic distribution of information	(92) 33.8%	(120) 44.1%	(60) 22.1%	(0) 0.00%	3.12
Procedures to monitor system use	(88) 32.4%	(120) 44.1%	(64) 23.5%	(0) 0.00%	3.09
Average Mean for Information Integrity					**3.12**
Information Availability	**VH**	**H**	**L**	**VL**	**Mean**
Procedures for handling and storing information	(72) 26.5%	(172) 63.2%	(28) 10.3%	(0) 0.00%	3.16
Existence of a guideline for physical media in transit that contains information	(56) 20.6%	(164) 60.3%	(52) 19.1%	(0) 0.00%	3.01
The activities of system administrators and system operators are being logged	(84) 30.9%	(128) 47.1%	(60) 22.1%	(0) 0.00%	3.09
Employees' activities are monitored under the existing legal framework	(72) 26.5%	(140) 51.5%	(60) 22.1%	(0) 0.00%	3.04

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

Monitoring the use of resources in computer systems is performed	(96) 35.3%	(112) 41.2%	(64) 23.5%	(0) 0.00%	3.12
Average Mean Information Availability					**3.08**
Weighted Mean for Information Security					**3.10**

Source: *Field survey, 2025*

Decision Rule: Very Low =1.00-1.74, Low =1.75-2.49, High =2.50-3.24, Very High=3.25-4.00

Key: VH=Very High, H=High, L=Low, VL=Very Low.

The examination of Table 1 above indicates that employees assessed the organization's information security protocols favourably, albeit with discrepancies in confidentiality, integrity, and availability. Concerning secrecy, over half of the respondents (143; 52.6%) concurred to a significant degree that there are protocols for the acceptance of new information systems, with 39.3% (107) assigning it a very high rating. A minuscule minority assigned a low rating (21; 7.7%) or a very low rating (1; 0.4%). Likewise, a majority of employees (184; 67.6%) reported a significant presence of a network operating guideline; nevertheless, only 14.7% (40) evaluated it as very high, while 17.6% (48) perceived it as low, highlighting a disparity in perception. The safeguarding of system documentation elicited robust feedback, with 148 respondents (54.4%) assigning a high rating and 84 (30.9%) designating it as very high. Confidentiality received an average score of 3.10, classified as strong.

Regarding information integrity, 164 employees (60.3%) assessed the separation of development, testing, and operating facilities as high, and 68 employees (25%) ranked it as very high, whereas only 14.7% (40) rated it bad. Concerning unauthorized software usage, 160 respondents (58.8%) evaluated it as high, 60 (22.1%) as extremely high, while 52 (19.1%) assessed it as low. The highest score for integrity was attributed to the presence of a backup policy, with 112 respondents (41.2%) rating it very high and 124 (45.6%) high, indicating widespread confidence in data security. In contrast, electronic messaging security and system usage oversight garnered comparatively lower evaluations, with more than one-fifth of employees evaluating them poorly (60; 22.1% and 64; 23.5%, respectively). Notwithstanding this, data integrity got the highest overall dimension score, averaging 3.12.

Regarding information availability, the management and storage of information received substantial endorsement, with 172 employees (63.2%) evaluating it as high and 72 (26.5%) as very high. The logging of system administrator activity received favourable ratings, with 128 individuals (47.1%) ranking it as high and 84 individuals (30.9%) rating it as very high. Nevertheless, the requirements for physical media in transit received comparatively less endorsement: 164 individuals (60.3%) evaluated it as high, 56 individuals (20.6%) rated it as very high, and 52 individuals (19.1%) regarded it as low. Likewise, around 23.5% of respondents (64 individuals) assessed the monitoring of resource utilization in computer systems as inadequate. Overall, the average availability was 3.08, categorizing it as high.

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 123-136)

www.abjournals.org

Research Question Two: What are the data handling stages practiced among Non-Academic Staff in Oyo State-owned Polytechnics?

Table 2: Data handling stages among Non-Academic Staff in Oyo State-owned Polytechnics.

Data handling stages	**SA**	**A**	**D**	**SD**	**x**
Data Creation					
Process of documenting academic data	(0) 0.0%	(268) 98.5%	(4) 1.5%	(0) 0.00%	2.99
Existence of a license that describes how data is used	(0) 0.0%	(236) 86.8%	(36) 13.2%	(0) 0.00%	2.87
Filing plans are created to least primary data used by functional units	(0) 0.0%	(240) 88.2%	(28) 10.3	(4) 1.5%	2.87
Average Mean for Data Creation					**2.91**
Data Classification	**SA**	**A**	**D**	**SD**	**x**
Process for archiving data in a repository for long-term storage	(0) 0.0%	(240) 88.2%	(32) 11.8%	(0) 0.0%	2.88
Practice of assigning a permanent identifier to your datasets	(0) 0.0%	(228) 83.8%	(36) 13.2%	(8) 2.9%	2.81
Data created by you is appropriately cited	(0) 0.0%	(236) 86.8%	(36) 13.2%	(0) 0.00%	2.87
Average Mean for Data Classification					**2.85**
Data Scheduling and Maintenance	**SA**	**A**	**D**	**SD**	**X**
Inclusion of a data availability statement in your manuscripts	(0) 0.0%	(224) 82.4%	(48) 17.6%	(0) 0.00%	2.82
Documenting data for easy understanding	(0) 0.0%	(264) 97.1%	(8) 2.9%	(0) 0.00%	2.97
Data retention schedule is in place	(0) 0.0%	(256) 94.1%	(16) 5.9%	(0) 0.00%	2.94
Average Mean for Data Scheduling and Maintenance					**2.91**
Use of Information	**SA**	**A**	**D**	**SD**	**x**
The institution addresses data privacy and security issues	(0) 0.0%	(256) 95.6%	(16) 5.9%	(0) 0.00%	2.94
Information verification before using for your decision-making	(0) 0.0%	(264) 97.1%	(8) 2.9%	(0) 0.0%	2.97

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

Average Mean for Use of Information	**2.95**
Weight Mean for Data handling stages	**2.89**

Source: *Field survey, 2025*

Decision Rule: Very Low =1.00-1.74, Low =1.75-2.49, High =2.50-3.24, Very High=3.25-4.00.

The analysis shown in Table 2 above indicates that the overall level of data handling stages among Non-Academic Staff in Oyo State-owned Polytechnics is moderate, with a weighted mean of 2.89. For the data creation dimension, most respondents (268; 98.5%) agreed that there is a process for creating metadata and documentation, resulting in a high mean of 2.99 and low variability (SD = 0.121), indicating strong consensus. Similarly, 236 staff members (86.8%) affirmed the existence of licensing procedures for data use and reuse, though 36 (13.2%) disagreed, leading to a slightly lower mean of 2.87 with a standard deviation of 0.339. Regarding the organizational file plan, 240 respondents (88.2%) agreed, while 28 (10.3%) disagreed and 4 (1.5%) strongly disagreed, resulting in a mean of 2.87 and variability of 0.380. The average for this dimension was 2.91, reflecting moderate implementation.

In terms of data classification, results were the weakest overall, with an average mean of 2.85. For example, 240 staff (88.2%) agreed on the existence of archiving processes, while 32 (11.8%) disagreed, producing a mean of 2.88 and a standard deviation of 0.323. Only 228 respondents (83.8%) acknowledged assigning permanent identifiers to datasets, while 36 (13.2%) disagreed and 8 (2.9%) strongly disagreed, giving the lowest mean (2.81) and the highest variability (SD = 0.463) among all items. Similarly, 236 (86.8%) supported the notion that data created by staff are appropriately cited, though 36 (13.2%) disagreed, resulting in a mean of 2.87 with a standard deviation of 0.339. These findings suggest that while data archiving and citation practices are moderately applied, systematic classification using permanent identifiers remains a weak point.

In the area of data scheduling and maintenance, the average mean was 2.91, indicating a moderate but near-high level of compliance. A total of 224 respondents (82.4%) agreed that a data availability statement is included in manuscripts, while 48 (17.6%) disagreed, yielding a mean of 2.82 and a standard deviation of 0.382. However, planning and organizing data, code, and supporting files showed stronger results, with 264 respondents (97.1%) agreeing and only 8 (2.9%) disagreeing, leading to a mean of 2.97 and low variability (SD = 0.169). Similarly, 256 respondents (94.1%) confirmed the presence of a documented data retention schedule, while 16 (5.9%) disagreed, resulting in a mean of 2.94 and a standard deviation of 0.236.

The use of information dimension achieved the highest average score (2.95), indicating stronger adherence compared to other areas. In terms of data privacy and security, 256 staff (95.6%) agreed, while 16 (5.9%) disagreed, resulting in a mean of 2.94 and SD of 0.236. The ability to evaluate the credibility of information sources was supported by 260 respondents (94.1%), while 8 (1.5%) disagreed and 4 (2.9%) strongly disagreed, giving a mean of 2.93 and SD of 0.357. Finally, verification of information before use had one of the highest agreement levels, with 264 staff (97.1%) supporting and only 8 (2.9%) disagreeing, producing a mean of 2.97 and SD of 0.169.

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 123-136)

www.abjournals.org

Test of Hypotheses

$H_0$1: There is no significant influence of data handling stages on information security among Non-Academic Staff in Oyo State-owned Polytechnics.

Table 3a: Influence of data handling stages (Data Creation, Data Classification, Data Scheduling, Maintenance, and Use of Information) on Information Security among Non-Academic Staff in Oyo State-owned Polytechnics

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.421[a]	.177	.165	.37041

a. Predictors: (Constant), Use of Information, Data Creation, Data Classification, Data Scheduling Maintenance

Table 3b:

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.896	4	1.974	14.386	.000[b]
	Residual	36.634	267	.137		
	Total	44.530	271			

a. Dependent Variable: Information Security Practice
b. Predictors: (Constant), Use of Information, Data Creation, Data Classification, Data Scheduling Maintenance

Table 3c:

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.639	.533		1.199	.232
	Data Creation	-.037	.134	-.016	-.273	.785
	Data Classification	.360	.111	.206	3.251	.001
	Data Scheduling Maintenance	.851	.158	.353	5.383	.000
	Use of Information	-.314	.154	-.130	-2.035	.043

a. Dependent Variable: Information Security Practice

In Table 3a, the correlation coefficient (R = .421) shows a moderate positive relationship between data handling stages components (data creation, data classification, data scheduling and maintenance, and use of information) and information security practices. The coefficient of determination (R^2 = .177) indicates that approximately 17.7% of the variance in information security practices can be explained by the combined effect of data handling stages dimensions. The adjusted R^2 (.165) confirms that after accounting for model complexity, about 16.5% of the variation remains attributable to these predictors.

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 123-136)
www.abjournals.org

Table 3b further confirms the model's overall significance, with the regression model yielding an F-value of 14.386 at $p < .001$. This suggests that the joint influence of the four data handling stages dimensions on information security is statistically significant. Thus, the null hypothesis (H_{01}) is rejected, and it can be concluded that data handling stages significantly influences information security among Non-Academic Staff.

The individual predictors in Table 3c reveal varied contributions. Data classification ($\beta = .206$, $t = 3.251$, $p = .001$) and data scheduling and maintenance ($\beta = .353$, $t = 5.383$, $p < .001$) were both positive and significant predictors, meaning improvements in these areas directly enhance information security practices. Conversely, use of information ($\beta = –.130$, $t = –2.035$, $p = .043$) showed a negative but significant influence, suggesting that while staff verify and use information, inconsistencies or possible misuse of information-related processes may reduce the effectiveness of security practices. Data creation ($\beta = –.016$, $t = –0.273$, $p = .785$), however, was not a significant predictor, implying that metadata documentation, licensing, and file planning in their current form do not meaningfully impact security outcomes.

The regression results demonstrate that data handling policies significantly influence information security practices, accounting for nearly one-fifth of their variance. Among the predictors, data scheduling and maintenance emerged as the strongest determinants, followed by data classification, while use of information had a negative contribution, and data creation had no significant effect. These findings imply that strengthening structured data management schedules and classification systems would yield the most improvement in safeguarding institutional information security.

DISCUSSION OF FINDINGS

The analysis of information security practices among Non-Academic Staff in Oyo State-owned Polytechnics reveals encouraging insights. With an overall weighted mean score of 3.10, it is clear that staff members generally recognize the importance of existing security protocols. Notably, there's strong support for safeguarding system documentation and adherence to backup procedures, which are crucial for maintaining data integrity. These findings support some findings investigated by some scholars on Digital Collaborative Tools, Strategic Communication, and Social Capital, Information security environment, culture, and legislation, Cybersecurity breaches and improvement of the quality of large-scale educational assessments, and a primer on insider threats in cybersecurity[1,2,3,4]. However, the findings also highlight some areas for improvement. Discrepancies emerged, particularly in monitoring system usage and managing unauthorized software, where responses were less favorable. This suggests that while staff are aware of their responsibilities, there's a need for further training and awareness programs to help them navigate the complexities of modern information security challenges effectively.

When it comes to data handling policies, the overall implementation was rated as moderate, with a weighted mean of 2.89. While Non-Academic Staff showed an understanding of data creation processes, weaknesses were identified in systematic classification and effective archiving practices. This points to the importance of establishing clearer guidelines and structured protocols that can enhance data management and minimize risks related to data breaches. These findings support some investigations by scholars on best practices to

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

encourage girls' education in Maiha local government area of Adamawa state in Nigeria, data privacy laws and compliance, attribute-based approaches for Secure Data Sharing in Industrial Contexts, and the effect of data protection frameworks against cybercrimes on cybersecurity in Nigeria.

Implication to Research and Practice

The findings carry significant implications for both research and institutional practice. The positive perception of information security among Non-Academic Staff in Oyo State-owned Polytechnics, indicated by a mean score of 3.10, reflects growing awareness and compliance with security protocols. This suggests that institutional efforts toward promoting information protection are producing encouraging results. The emphasis on safeguarding system documentation and maintaining backups demonstrates a sound understanding of data integrity principles. These outcomes align with existing studies on digital collaboration, strategic communication, and cybersecurity environments, confirming that staff awareness is essential to building a secure institutional framework. However, weaknesses in system monitoring and unauthorized software control point to ongoing challenges in translating awareness into consistent practice. This calls for targeted training programs, stronger policy enforcement, and improved technical supervision. The moderate performance in data handling (mean score 2.89) further reveals gaps in data classification and archiving, suggesting the need for clearer data management guidelines and structured procedures. Poor documentation practices increase risks of data loss and undermine accountability. Overall, the findings highlight both progress and areas needing attention. They emphasize the importance of combining policy clarity, staff development, and technological investment to strengthen institutional information security. Academically, the results enrich ongoing discussions on how organizational culture and staff behavior influence cybersecurity effectiveness in public educational settings.

CONCLUSION

This study has yielded significant insights into the relationship between data handling stages and information security practices among Non-Academic Staff in Oyo State-owned Polytechnics, Nigeria. The findings reveal a high level of information security practices. This positive outcome reflects a commendable awareness among staff regarding the necessity of protecting sensitive institutional data. Particularly, the study also indicated that Non-Academic Staff show strong practices in critical areas like safeguarding of system documentation and adherence to backup protocols. However, the study also identified gaps, particularly in the monitoring of system usage and the management of unauthorized software, which received comparatively lower evaluations. This highlights an urgent need for enhanced training and awareness programs aimed at equipping staff with the skills necessary to navigate the complexities of modern information security challenges.

In terms of data handling policies, the findings showed an overall implementation level assessed as moderately high. While Non-Academic Staff demonstrated a solid understanding of data creation processes, there were notable weaknesses in systematic data classification and effective archiving practices. This suggests that while the foundations for effective data management exist, further efforts are required to establish clearer guidelines and structured protocols. Such improvements are essential not only for compliance with regulatory

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

frameworks but also for the protection of sensitive information that is crucial to the institution's operational integrity.

FUTURE RESEARCH

Based on the findings of this study, future researchers are encouraged to;

1. Explore the same topic using alternative theoretical frameworks beyond those employed in this study.
2. Consider investigating other variables aside from data handling stages, access control, and information management, focusing on aspects beyond information security.
3. Conducted same or related study in different geographical areas other than those examined in this research to enhance the generalizability of the findings.
4. Investigating the impact of technological advancements, such as artificial intelligence.

REFERENCES

Adenekan, T. E., & Ologbosere, O. A. (2021). *Information security policy and practices among office managers in the telecommunications industry in Nigeria*. International Journal of Advanced Research in Multidisciplinary Studies (IJARMS), 1(1), 70–78.

Ahmadi, S. (2024). *Zero trust architecture in cloud networks: Application, challenges, and future opportunities.* Journal of Engineering Research and Reports, 26(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i2517

Aladesanmi, O., Afolabi, B., & Oyebisi, T. O. (2012). *Assessing network services and security in Nigerian universities.* Journal of Computer Science and Information Technology (JCSIA), 19(1), 60–66. https://doi.org/10.4314/JCSIA.V19I1.8

Ameer, S., Benson, J., & Sandhu, R. (2022). *An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach*. Information, 13(2), 60. https://doi.org/10.3390/info13020060

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). *Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations.* Computer Science & IT Research Journal, 5(3), 528–543.

Barata, K., Bennett, R., Cain, P., & Routledge, D. (2001). *From accounting to accountability: Managing financial records as a strategic resource. Namibia: A case study. London*: International Records Management Trust.

Boopathi, S. (2023). *Securing healthcare systems integrated with IoT. In IGI Global* (pp. 186–209). https://doi.org/10.4018/978-1-6684-6894-4.ch010

El Filali, C., Bourian, I., & Chougdali, K. (2024). *Privacy-preserving and access control scheme for IoT-based healthcare systems using Ethereum blockchain*. IEEE Communications Network, 1–6.

El Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2019). *A survey on access control mechanisms for cloud computing. Transactions on Emerging Telecommunications Technologies*, 1(2), 31. https://doi.org/10.1002/ett.3668

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4

Flynn, S. J. A. (2001). *The records continuum model in context and its implications for archival practice.* Journal of the Society of Archivists, 22(1), 79–93. https://doi.org/10.1080/00379810120055401

International Records Management Trust (IRMT). (2009). *Managing personnel records in an electronic environment: TERM project. London:* IRMT. https://www.irmt.org

Krejcie, R.V. (1970), University of Minnesota, Duluth. Daryle W. Morgan, Texas A and M. University.

Marshall, P. (2000). Life cycle versus continuum: *What is the difference? Informa Quarterly: Records Management Association of Australia*, 16(2), 20–25.

Nyame, G., & Qin, Z. (2020). P*recursors of role-based access control design in KMS: A conceptual framework.* Information, 11(6), 334. https://doi.org/10.3390/info11060334

Yang, B. (2023). *Enforcement of separation of duty constraints in attribute-based access control.* Computers & Security, 131, 103294. https://doi.org/10.1016/j.cose.2023.103294

Article DOI: 10.52589/BJCNIT-WMFXRIE4
DOI URL: https://doi.org/10.52589/BJCNIT-WMFXRIE4