Chapter One

Introduction

1.1 Background to the Study

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. In academic environments, especially institutions such as the Oyo State-owned polytechnics, a wide range of services, including student records, admission data, departmental information, grades, transcripts, certificates, staff profiles, academic programs, and institutional achievements, have been digitized. Some of these systems are also being considered for further automation. Ensuring the protection of these digital services has become a critical responsibility within the broader information management infrastructure of such institutions.

Information security refers to the strategic effort to shield data from threats that could compromise its privacy, accuracy, or accessibility. It involves using tools and techniques such as encryption, user authentication, and firewalls to prevent unauthorized access, tampering, or loss of information. These safeguards ensure that data remains trustworthy and available for both academic and administrative functions. At its core, 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[1]. Organizational data must be carefully guarded to maintain its privacy, accuracy, and accessibility. Depending on its nature, some information may demand protection on several

Lead City University Ibadan DO NOT COPY

fronts, highlighting the varied requirements involved in managing and securing data across different areas of an organization[2]. The foundation of information security consists of the three properties which are confidentiality, integrity and availability[3]. 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. The foundational pillars of information security, as outlined in the widely recognized CIA triad, are confidentiality, integrity, and availability[4]. 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.

In developing nations like Nigeria, academic institutions often encounter significant hurdles when it comes to implementing effective information security. These challenges include a shortage of qualified professionals, limited financial resources, cultural factors, and outdated infrastructure and equipment, among others[5]. Furthermore, information security programs in many academic institutions in developing countries are not part of strategic plans nor are they operational, they lack documentation, and lack benchmarking[5]. A major obstacle to effective information security in academic institutions across Nigeria, including those in Oyo State is the limited awareness among users and a general lack of a security-conscious culture. Many institutions in developing countries still operate without formalized strategies for safeguarding information, and often lack essential components like data backup systems and continuity plans for their IT infrastructure. Additionally, the cost of delivering proper training and raising awareness around information security is considered high, making it difficult to implement on a wide scale. Other contributing factors include cultural influences, insufficient

Lead City University Ibadan DO NOT COPY

support from leadership, tight budgets, uncoordinated security policies, and low motivation among Non-Academic Staff, all of which hinder the successful rollout of information security initiatives in these academic settings[6]. In Oyo State-owned polytechnics, enforcement against cyber-related offenses remains notably weak. This is largely attributed to limited expertise among law enforcement personnel in handling digital crimes, coupled with systemic issues such as corruption and the absence of robust legal frameworks specifically addressing information system violations[7]. In academic settings where efforts toward democratization are minimal and ICT infrastructure remains underdeveloped, concerns around privacy, data protection, and confidentiality often receive little attention or priority. This lack of emphasis has played a significant role in the ongoing information security challenges experienced by state-owned polytechnics in Oyo State, Nigeria.

Contrary in the developed nations, information security has been enhanced through many means like appropriate policy implementation, technology utilization, and practices aimed at protecting data and information systems. Developed nations also implemented advanced cybersecurity frameworks, such as the ISO/IEC 27001 standards, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the European Union's General Data Protection Regulation (GDPR) which establishes a standard for personal data protection. Nevertheless, despite these advancements, cyber threats continue to evolve at a rapid pace. Ransomware and data breaches have become ongoing threats, shifting information security from a technical issue to a wider geopolitical and economic challenge. With an increased dependence on the information management system connected over open data networks, efficient information security has become a crucial success feature for academic institutions in the developed and developing countries.

Lead City University Ibadan DO NOT COPY

In Africa, the digital transformation is accelerating, driven by enhanced mobile connectivity, innovations in financial technology (fintech), and broader internet access. While these advancements provide promising opportunities for growth and inclusion, they also introduce new vulnerabilities within the information ecosystem. The continent faces considerable challenges, including inadequate cybersecurity infrastructure, a shortage of specialized personnel, and limited public awareness. However, there are indications of progress. The African Union's Convention on Cyber Security and Personal Data Protection, aims to unify cybersecurity legislation among member states. Nations such as Kenya, South Africa, and Egypt have implemented national cybersecurity policies and data protection laws, reflecting an increasing recognition of the necessity for digital protection. Yet, the execution of these measures remains uneven, and numerous countries continue to grapple with balancing security, and accessibility.

A factor that could enhance 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, it is central in the administration of institutions of learning because it documents the planning and implementation of appropriate course of services allowing proper monitoring of work[8]. 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[9]. 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

Lead City University Ibadan DO NOT COPY

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[10].

Data are important historical and legal tools and are necessary for the smooth running of an academic institution. Data constitute an essential instrument of administration without which operational processes and functions cannot be executed. For example, a successor to a position needs available records to find his bearing when he takes over from another or when he has to fill vacancy created by resignation, transfer, retrenchment or death. Using such data as a springboard, the successor can decide on whether to continue with, modify or change certain techniques or practices. Data play immeasurable roles in administration because managers, administrators and Non-Academic Staff employ them on routine basis for carrying out diverse administrative duties especially in decision making and record processing and management[11]. The information contained in data helps to enlighten and educate administrators on issues relevant to the institution. Data are also used as important sources for strategic planning and successful implementation as well as good policy formulation and implementation.

In addition, data are primary sources of information for research, which can serve as reference, as well as evidence. Decision-making in an academic institution is an administrative function and invariably requires information in the form of data. Information is very vital to any decision-making, while decision-making is the backbone of managerial as well as administrative functions, this is because decisions direct actions. Good and effective decisions can only be made when the right information is made available at the right time to the right recipient. Data handling stages in Polytechnics today need to pay more attention to the management of data in the custody of Non-Academic Staff for efficiency and effectiveness. Information in form of data reduces uncertainties and facilitates decision-

Lead City University Ibadan DO NOT COPY

making. Polytechnic possesses huge amounts of data which includes correspondences, accounting documents, personnel files, pay roll, minutes of meetings (senates, polytechnic council, faculty and departmental boards meetings) students' registration, students' admissions and examination records, inventory of facilities, budgetary information, list of courses offered, time-tables for lectures, speeches, legal documents, deeds, financial records, letters (appointment, confirmations, admissions, sick leave, queries) and so forth.

Accurate and timely availability and use of the data on these would reduce the common problems of management in polytechnics, such as difficulty in finding information needed to take a decision or to respond to inquiry, delays in payment of staff emoluments and fringe benefits, piling up of administrative matters causing discontent among staff, students, parents etc., improperly registered students in school registers and records, inaccurate demographic figures resulting in either lack of places/spaces for students or wastage of spaces/places available and inability to forward students reports/records or release results on schedule[12].

The idea of data handling stages has to do with the control of data passing out of current and semi-current stages into archival care. 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[13]. Data creation is the process of generating new data or information, either manually or automatically, through various methods such as collecting, recording or synthesizing. It involves producing raw data from sources like user input, sensors, simulations or digital processes, which can then be used for analysis, storage, or decision making. Examples include entering data into a database, generating logs from software, or creating synthetic datasets for testing.

Data classification is the process of organizing data into categories or groups based on specific criteria such as sensitivity, type, of purpose, to facilitate management, security and

Lead City University Ibadan DO NOT COPY

access control. It involves labelling or tagging data (data like public, confidential, or sensitive) to ensure proper handling, storage, and compliance with regulations. Data scheduling refers to the process of planning and automating the timing of data with related tasks such as collection, processing, or transfer. It involves setting specific intervals or triggers for tasks to ensure data is updated, backed up, or processed efficiently.

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. To guarantee efficiency, effectiveness and to enable organizations like polytechnics to survive in the accountability period in which we live, data must be actively managed throughout their life. This needs to be done via a data management programme which is the main implementation vehicle for the data handling stages whose aims and objectives must be aligned with those of the organization to which it refers[14]. In order to make academic and administrative data of Oyo State-owned Polytechnics secured, access must be restricted to only the authorized staff.

Data is increasingly becoming the cornerstone of academic operations; hence, securing databases against insider threats poses a significant challenge. Insider threats from individuals within the institution present a unique and complex risk to database security[15]. These threats include malicious actions aimed at data theft, sabotage, or unintentional breaches due to negligence or lack of awareness. Traditional security measures often fail to effectively address insider threats due to their internal origin and the abusers' potential access and knowledge of the system. Role-Based Access Control (RBAC) has been

Lead City University Ibadan DO NOT COPY

recognized as a promising approach to mitigate these threats by restricting access to sensitive information based on users' roles within an institution[16].

A system administrator's mistake could occur due to inadequate training on cloud security protocols and may result in a misconfiguration that leaves sensitive data vulnerable. This incident underscores the potential consequences of human error in cloud environments, highlighting the need for a comprehensive approach to data security. While some experts argue that such errors stem from insufficient training, others contend that the incident underscores the need for adequate security measures, such as RBAC. RBAC operates on the principle of least privilege where users are assigned roles with specific permissions mapped to their job responsibilities. If RBAC is implemented, it would have significant effect in order to reduce data damage by limiting access based on job functions, granting only authorized employees' access to view sensitive information[17].

Traditional methods like employee monitoring can play a role, these cases highlight the necessity of more comprehensive strategies like Role-Based Access Control (RBAC), which offers a more robust line of defense. These incidents collectively underscore the necessity of a study focusing on RBAC's potential to fortify database security against insider threats. Critical weaknesses in current security practices among Non-Academic Staff of Oyo State-owned polytechnics include inadequate termination procedures, insufficient user access reviews, and the lack of proactive monitoring for suspicious activities. However, the efficacy of RBAC in real-world applications is hindered by challenges in accurate role definition, dynamic access needs, and the evolving nature of insider threats[18]. Moreover, the lack of comprehensive research on the specific impact of RBAC on mitigating insider threats leaves a gap in understanding its effectiveness and areas for improvement.

This study addresses this gap by examining how RBAC can be optimized to counter insider

Load City University Ibadan DO NOT COPY

threats more effectively and reduce data access to only the authorized staff (Non-Academic Staff). It proposes a nuanced understanding of RBAC's role in enhancing database security and identifying strategies to overcome its implementation challenges[18]. Without such an investigation, these polytechnics may continue to face significant risks from insider threats, undermining their operational integrity, data confidentiality, and competitive advantage. While examining and proposing enhancements to RBAC frameworks, the study aims to address these vulnerabilities, offering institutions robust strategies to protect their valuable data assets against the ever-present risk of insider threats. In view of the perceived challenges observed about information security, data handling stages, and access control, this study intends to investigate data handling stages, access control and information security practice among non-academic staff in State-owned Polytechnics, Oyo State, Nigeria.

1.2 Statement of the Problem

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. When the level of information security is high, all stakeholders can feel secure knowing their data is protected. However, 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 and access control have therefore been identified as key factors influencing information security among Non-Academic Staff in these institutions.

Data handling stages is crucial for information security, it set clear procedures for managing and safeguarding data. Access control is equally important for information security as it

Lead City University Ibadan DO NOT COPY

regulates who can view or use data, helping to prevent unauthorized access and data leaks. However, several research studies have been carried out on Information Security, Information handling stages, authorization and access control policies, and access control for trusted data sharing[19,20,21,22]. However, there is a scarcity of literature on data handling stages, access control, and information security. Therefore, this study examines the influence of data handling stages and access control on information security practices among non-academic staff in State-owned polytechnics, Oyo State, Nigeria.

1.3 Aim and Objectives of the Study

The aim of this study is to investigate data handling stages, access control and information security among non-academic staff in State-owned polytechnics, Oyo State, Nigeria. The specific objectives are to:

i. assess the level of information security practice by non-academic staff in State-owned polytechnics, Oyo State, Nigeria
ii. examine the data handling stages that exist in State-owned polytechnics, Oyo State, Nigeria
iii. identify the level of access control by non-academic staff of State-owned Polytechnics in Oyo State, Nigeria
iv. determine the influence of data handling stages on information security practice among non-academic staff in State-owned Polytechnics, Oyo State, Nigeria
v. ascertain the influence of access control on information security practice among non-academic staff in State-owned polytechnics, Oyo State, Nigeria
vi. determine the combined influence of data handling stages and access control on information security practice among non-academic staff in State-owned polytechnics, Oyo State, Nigeria

Lead City University Ibadan DO NOT COPY

1.4 Research Questions

The following research questions guided the study:

1. What is the level of information security practiced by Non-Academic Staff in State-owned Polytechnics, Oyo State, Nigeria?
2. What are the data handling stages practiced by Non-Academic Staff in State-owned Polytechnics, Oyo State, Nigeria?
3. What is the level of access control practiced by non-academic staff in State-owned Polytechnics, Oyo State, Nigeria?

1.5 Research Hypotheses

The following hypotheses were formulated and tested at 0.05 level of significance:

$H_0$1: There will be no significant influence of data handling stages on information security among non-academic staff in State-owned polytechnics, Oyo State, Nigeria.

$H_0$2: There will be no significant influence of access control on information security among non-academic staff in State-owned polytechnics, Oyo State, Nigeria.

$H_0$3: There will be no significant combined influence of data handling stages and access control on information security among non-academic staff in State-owned polytechnics, Oyo State, Nigeria.

1.6 Significance of the Study

This research work will be significant and of great benefit to various stakeholders, including the management of State-owned polytechnics, non-academic staff, students, researchers and polytechnics regulatory body (NBTE). This study will greatly assist institutional management in formulating and executing robust policies designed to ensure the protection of organizational data. Specifically; it will assist management team in establishing effective

Lead City University Ibadan DO NOT COPY

access control protocols, provisioning appropriate technological infrastructure, and instituting rigorous training and capacity-building programs for registry personnel. These measures are important for ensuring the confidentiality, integrity, and availability of both academic and administrative information of all stakeholders. Putting these components into institutional practice, non-academic staff will be well-equipped to perform their administrative duties with heightened awareness and diligence. The presence of clear guidelines, adequate resources, and continuous professional development will foster a sense of motivation and accountability among staff members. Consequently, they will be more inclined to adhere to established security protocols and exercise caution in the handling of sensitive information, thereby reinforcing a culture of data protection and operational excellence within the institution.

Beyond the contributions to institutional policy and infrastructure, this study will play a critical role in enhancing the operational capacity of non-academic staff by equipping them with foundational and advanced competencies across a wide range of administrative functions. It will provide targeted guidance and practical frameworks for improving proficiency in student record management, including the accurate documentation, retrieval, and updating of academic records in compliance with institutional and regulatory standards. Moreover, the study will address best practices in registration and enrollment procedures, ensuring that staff are well-versed in managing admission workflows, verifying student eligibility, and maintaining real-time enrollment data. It will also offer insights into the efficient handling of transcript issuance, emphasizing the importance of data accuracy, confidentiality, and timely delivery to support academic mobility and graduate verification.

In the domain of examination support, the study will outline protocols for coordinating exam schedules, managing invigilation logistics, and securely processing results. It will further explore data management strategies, including the use of digital platforms for storing,

Lead City University Ibadan DO NOT COPY

analyzing, and reporting institutional data, thereby fostering a data-driven culture within the registry unit. Additionally, the study will highlight the significance of liaison roles, preparing staff to serve as effective intermediaries between students, faculty, and administrative departments. This includes cultivating strong communication skills, conflict resolution techniques, and a service-oriented mindset. Administrative activities such as filing, correspondence, scheduling, and compliance reporting will also be addressed, ensuring that staff are equipped to maintain operational efficiency and uphold institutional standards. Collectively, these enhancements will not only improve the quality and reliability of registry services but also contribute to the professional development and job satisfaction of staff members.

This study will also make a meaningful contribution to the protection of student interests by reinforcing the principles of confidentiality and authenticity in academic progression. Through establishing secure protocols for data handling and access control, the study will ensure that students' academic records, including registration details, examination results, and transcript information, are managed with strict adherence to privacy standards. This will prevent unauthorized access, manipulation, or disclosure of sensitive information, thereby safeguarding the integrity of each student's academic journey. Furthermore, the study will promote transparency and accountability in record-keeping practices, ensuring that all academic documentation reflects genuine achievements and verifiable credentials. Such measures are essential not only for maintaining institutional credibility but also for fostering student trust in the administrative processes that govern their academic development. Ultimately, the study will help create a secure and trustworthy environment in which students can pursue their education with confidence, knowing that their personal and academic data are protected and accurately represented.

Lead City University Ibadan DO NOT COPY

The study is also significant as it serves as a guide for future researchers in both private and government polytechnics to understand the necessary electronic resources and skills to enhance information security, access control, and compliance with data handling policies. And since this study is based on current events that are still unfolding, it is expected to provide relevant and up-to-date information for scholars and students researching various aspects of information security, data handling policies, and access control.

In many ways, this study will serve as a valuable resource for the National Board for Technical Education (NBTE) in Nigeria, particularly in the formulation and refinement of regulatory frameworks governing institutional data governance. Through the provision of empirical insights and contextual analysis, the study will inform the development of full policies that address key dimensions of information security, including data confidentiality, integrity, and availability across technical and vocational institutions in Nigeria. Specifically, the study will offer guidance on the delineation of data handling stages from acquisition and processing to storage, transmission, and disposal, ensuring that each phase is governed by standardized protocols that mitigate risks and promote accountability. Furthermore, it will support the establishment of comprehensive access control mechanisms, enabling institutions to define user privileges, enforce authentication procedures, and monitor data usage in alignment with best practices and ethical standards. Through these contributions, the study will not only enhance institutional resilience against data breaches and cyber threats but also assist NBTE in aligning its regulatory mandates with global trends in educational data management. Ultimately, the findings will empower the Board to enact policies that foster a secure, transparent, and efficient information ecosystem within Nigeria's technical education sector.

Lead City University Ibadan DO NOT COPY

1.7 Scope of the Study

This study covers data handling stages, access control and information security practice among non-academic staff in State-owned Polytechnics, Oyo State, Nigeria. The measures of information security are information confidentiality, information integrity, and information availability. The measures for data handling stages are data creation, data classification, data scheduling and maintenance and use of information. In contrast, the measures used for access control are roles definition, permissions allocation, session management and user assignments control, this four measures are selected as they are most suitable for the respondents and the study.

The geographical scope covers all Oyo State-owned Polytechnics which include The Polytechnic, Ibadan, Adeseun Ogundoyin Polytechnics, Eruwa and Oke-Ogun Polytechnics, Saki. The respondents are all non-academic staff in the institutions ranging from administrative (Deputy Registrars, Principal Assistant Registrars, Senior Assistant Registrars and Assistant Registrars), executive (Chief Executive Officers, Principal Executive Registrars, Senior Executive Officers, Executive Officers and Clerical Officers), health records officers, and secretarial (Chief Confidential Secretaries) cadres. These cadres are selected from the overall non-academic staff as they are closely dealing with data and information within the institution's settings.

1.8 Limitations of the Study

The main limitation faced in this study was a delay in obtaining approval to administer the research questionnaire. However, this challenge was eventually resolved through the persistent efforts and follow-up by the researcher and research assistants, and the study was successfully carried out. Another challenge encountered was respondents' fear regarding the

Lead City University Ibadan DO NOT COPY

confidentiality of the information they provided. This was addressed by assuring them that their responses would be used strictly for academic purposes and that all identifying details would remain confidential.

1. 9 Operational Definition of Terms

Information Security: This is a way or practice through which information is protected from unauthorized access, disclosure, alteration, and destruction in State-owned polytechnics, Oyo State, Nigeria. Information security will be measured by Information confidentiality, integrity and availability.

Information Confidentiality: This involves protecting sensitive or private data from unauthorized access, disclosure, or use by Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria.

Information Integrity: This refers to the accuracy, completeness, and reliability of data, ensuring it remains unaltered and trustworthy throughout its life cycle among the Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria.

Information Availability: This is the assurance that data and systems are accessible and operational to authorized Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria.

Data Handling Stages: This set of procedures defines how non-academic staff in State-owned polytechnics, Oyo State, Nigeria collect, store, process, share, and dispose of data. It will be evaluated based on data creation, classification, scheduling, maintenance, and the use of information.

Data Creation: This is the process of generating new data through activities such as data entry, collection or system-generated outputs among Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria.

Lead City University Ibadan DO NOT COPY

Data Classification: This is the process of categorizing data based on its sensitivity, value, or criticality to Oyo State-owned Polytechnics.

Data Scheduling and Maintenance: This is the systematic planning and organization of data related tasks or processes to occur at specific time intervals among Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria.

Use of Information: This is the application or processing of data to achieve specific purposes such as decision making, analysis, communication or operational tasks among Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria.

Access Control: This is the security process of regulating who or what can view, use or modify data, systems, or resources in State-owned polytechnics, Oyo State, Nigeria. This will be measured by roles definition, permissions allocation control, session management, and user assignments control.

Roles Definition: This is a predefined set of permissions or privileges assigned to Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria, within a system to regulate their access to data, resources and functionalities.

Permissions Allocation Control: This is a specific right or privilege granted to Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria, within a system to perform actions on data.

Sessions Management: This is the process of managing and regulating Non-Academic Staff access to resources, systems, or data within Oyo State-owned Polytechnics.

User Assignments Control: This is the process of assigning specific roles to Non-Academic Staff in State-owned polytechnics, Oyo State, Nigeria, defining the level of access and privileges within the academic system of the institutions.

Non-Academic Staff: These are personnel in Oyo State-owned Polytechnics who are in charge of core administrative, secretarial and clerical activities other than academic duties.

Lead City University Ibadan DO NOT COPY

Endnotes

1. G. Nyame & Z. Qin. Precursors of Role-Based Access Control Design in KMS: A Conceptual Framework. **Information**. Jun. 2020;11(6):334.

2. T. E.,Adenekan, & O. A. Ologbosere. "Information Security Policy and Practices among Office Managers in Telecommunications Industry in Nigeria." **International Journal of Advanced Research in Multidisciplinary Studies (IJARMS)**, 1(1), 2021, 70-78

3. S. Ameer, J. Benson & R. Sandhu. An Attribute-Based Approach toward a Secured Smart-Home IOT Access Control and a Comparison with a Role-Based Approach. **Information**. 13(2), 2022, 60.

4. R. El Sibai, N. Gemayel, J. Bou Abdo & J. Demerjian. A Survey on Access Control Mechanisms for Cloud Computing. **Transactions on Emerging Telecommunications Technologies**. 1(2), 2019, 31.

5. T. Zaidi, M. Usman, M. Umar Aftab, H. Aljuaid & Y. Yasin Ghadi. Fabrication of Flexible Role-Based Access Control Based on Block Chain for Internet of Things use Cases. **ieeexplore.ieee.org;** 2023.

6. Computer Security Division. Role Engineering and RBAC Standards - Role Based Access Control, CSRC, CSRC. CSRC, NIST; Nov. 21, 2016.

7. R. A. Alsowail & T. Al-Shehari. A Multi-Tiered Framework for Insider Threat Prevention. **Electronics**. 10(9), 2021, 1005.

8. S.J.A. Flynn, "*The Records Continuum Model in Context and its Implications for Archival Practice*", **Journal of the Society of Archivists** 22(1), 2001, 79-93.

9. P. Marshall, "*Life Cycle Versus Continuum: What is the Difference?*" **Informaa Quarterly Records Management Association of Australia, Sydney**, 16 (2), 2000, 20-25.

10. B. Yang. *"Enforcement of Separation of Duty Constraints in Attribute-Based Access Control"*. **Computers and Security**. 131, 2023; 103294.

11. K. Ragothaman, Y. Wang, B. Rimal & M. Lawrence, "*Access Control for IOT: A Survey of Existing Research, Dynamic Policies, and Future Directions"*. **Sensors**. 23(4), 2023, 1805.

12. A. Chiquito, U. Bodin, & O. Schelen. Attribute Based Approaches for Secure Data Sharing in Industrial Contexts. **IEEE Access**. 11, 2023, 10180–10195.

13. S. Ahmadi. "*Zero Trust Architecture in Cloud Networks: Application, Challenges, and Future Opportunities"*. **Journal of Engineering Research and Reports**. 26(2), 2024, 215–228.

Lead City University Ibadan DO NOT COPY

14. S. Aboukadri, A. Ouaddah, & A. Mezrioui. "*Machine Learning in Identity and Access Management Systems: Survey and Deep Dive*". **Computers and Security**. 139, 2024, 103729.

15. S. O. Olabanji. "*AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems."* **Asian Journal of Research in Computer Science.** 17(3), 2024, 38–56.

16. K. Putch. "*Healthcare Security Services Firms Tackle Ransomware Spike TechTarget***.**" **IT Channel,** 2021. (accessed Mar. 30, 2024)

17. S. Deng et al. "*Cloud-Native Computing: A Survey from the Perspective of Services.*" **Proceedings of the IEEE.** 112(1), 2024, 12–46.

18. T. Baumer, M. Müller & Günther Pernul. "*System for Cross-Domain Identity Management (SCIM): Survey and Enhancement with RBAC*". **IEEE Access**. 11, 2023, 86872–86894.

19. M. S. Alraja, U. J. Butt & M. Abbod, *"Information Security Policies Compliance in a Global Setting: An Employee's Perspective."* **Journal of Computer and Security**, 129, 2023, 103208

20. Royal College of Arts, Information Handling Policy, Dec. 2024, https://www.rca.ac.uk/more/organisation/policies-and-codes-of-practice/information-handling-policy

21. M. Zubair et al., "*Access Control for Trusted Data Sharing,"* **EURASIP Journal on Information Security**, 2024, 30 https://doi.org/10.1186/s13635-024-00178-z

22. Science Direct, Access Control Policies, **Science Direct Journals**, https://www.sciencedirect.com/topics/computer-science/access-control-policies

Lead City University Ibadan DO NOT COPY

Chapter Two

Review of Related Literature

This chapter reviewed related literature for a better understanding of the research problem. The chapter is presented under the following headings:

2.1 Conceptual Review

2.1.1 Concept of Information Security

2.1.2 Concept of Data Handling Stages

2.1.3 Concept of Access Control

2.2. Theoretical Framework

2.2.1 TRIAD (CIA) Framework

2.2.2 Records Continuum Model

2.2.3 Role–Based Access Control (RBAC)

2.3 Review of Empirical Studies

2.3.1 Data Handling Stages and Information Security

2.3.2 Access Control and Information Security

2.4 Conceptual Model

2.5 Summary of the Reviewed Literature

Endnotes

Load City University Ibadan DO NOT COPY

2.1 Conceptual Review

2.1.1 Concept of Information Security

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, by limiting access to only those who are authorized; integrity, by ensuring the data remains accurate and unchanged; and availability, by keeping information accessible whenever it is needed. This comprehensive approach protects not just the data itself, but also the infrastructure that stores and processes it. Its relevance spans across various sectors, with higher education institutions placing particular emphasis on it. While offering a structured way to manage risks, information security enables organizations to tackle threats like cyberattacks and internal breaches, helping them maintain smooth operations and build trust[1].

Information security refers to the ongoing effort to defend both data and the systems that manage it from unauthorized access, misuse, exposure, disruption, or alteration. Because threats are constantly evolving, this field demands continuous attention and flexible strategies to stay ahead. Its process-driven nature encourages organizations to take proactive steps, such as conducting audits and assessing risks to strengthen their resilience against emerging challenges. For professionals in Information Technology governance and auditing, this approach is especially valuable. At its core, information security is a form of risk management. It focuses on identifying potential threats to digital assets and implementing practical solutions to reduce their impact. This hands-on methodology allows organizations to customize their security practices based on the sensitivity and importance of their data, helping them allocate resources wisely. It underscores the importance of prioritizing

Lead City University Ibadan DO NOT COPY

protection efforts based on the value and sensitivity of information, enhancing efficiency and effectiveness[2].

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. In today's digital age, information has evolved beyond its traditional role to become a vital resource that demands thoughtful handling and protection. The usefulness of information can be evaluated through several key factors. It must be relevant to the task at hand, supporting sound decision-making. Timing is also critical and information is most valuable when it is current and delivered promptly. Reliability hinges on its accuracy and clarity, while completeness ensures that all necessary details are available for proper understanding and application[2].

Security involves a wide range of methods and guiding principles aimed at safeguarding valuable assets from damage, unauthorized use, or potential loss[3]. Security as a concept has undergone major transformation over time, evolving to meet the demands of emerging threats brought on by technological progress. At its foundation, it involves taking preventive steps, building protective structures, and creating responsive strategies to counter potential risks. Today's approach to security goes far beyond basic defense, it embraces proactive methods like risk evaluation, threat analysis, and the design of robust systems that can withstand disruptions and maintain functionality. Effective security frameworks must address both physical and digital dimensions, recognizing how modern threats are often intertwined and how different areas of security influence one another.

Lead City University Ibadan DO NOT COPY

The origins of information security can be traced back to the early days of computer security. This discipline emerged in response to the increasing need to safeguard physical environments, computer systems, and software from threats such as theft, hacking attempts, and unauthorized access[3]. Information security is understood as the effort to maintain the privacy, accuracy, and accessibility of an organization's data assets[3]. The roots of information security can be traced back to World War II, a period that saw the development of the first mainframe computers used to decode enemy communications. To protect these machines and preserve the integrity of the sensitive data they handled, various security protocols were introduced. Among these were physical access controls, such as badges, keys, and the presence of security personnel who identified authorized individuals by sight[4]. As World War II unfolded, the need to safeguard sensitive data became increasingly evident. Beyond physical protection, there was a rising demand to secure the digital information stored on early computers from potential breaches or misuse. This urgency spurred progress in cryptographic techniques and the creation of stronger security protocols. The lessons learned during that era laid the groundwork for today's information security standards, which continue to adapt in response to technological growth and emerging threats. In the modern world, data protection is no longer limited to military operations, it is a critical concern across industries like business, healthcare, and even daily life, as digital systems now hold and transmit some of our most valuable information.

Information security has developed into a distinct field that bridges the gap between managing data and enforcing protective measures. Its primary goal is to safeguard valuable information at every stage of its existence, from the moment it is created, through its storage and transmission, all the way to its final disposal. As digital systems become more central to how individuals and organizations operate, the need for strong security practices continues to grow in response to increasingly sophisticated cyber threats. One of the core principles of this

Lead City University Ibadan DO NOT COPY

discipline is confidentiality, which ensures that sensitive information is only accessible to those with proper authorization. Achieving this requires the use of secure access controls, encryption technologies, and well-defined security protocols. However, these protective measures must be carefully balanced with the need for operational efficiency, allowing legitimate users to retrieve the information they need without compromising its safety[5].

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[6]. Information security is commonly understood through the lens of three core principles: confidentiality, integrity, and availability. As organizations around the world become increasingly reliant on digital systems, securing these information assets has become a pressing concern. Historically, efforts to protect data have leaned heavily on technological solutions like encryption tools, anti-malware software, and firewalls. However, relying solely on these measures is not enough. Research suggests that a significant portion, estimated between 50% and 70% of security breaches stem from human factors, including unintentional errors and deliberate misuse by employees. This highlights the need for a more comprehensive approach that addresses both technical and behavioral risks[7]. Enhancing information security requires a balanced investment in both technological tools and organizational strategies. In light of this, researchers and professionals have increasingly turned their focus toward the human side of security, drawing on concepts from behavioral science and social psychology to better understand and influence user behavior within digital environments[8]. In this context, raising employees' awareness about information security is a crucial foundation for fostering responsible security behavior. It significantly influences how well staff members adhere to organizational policies and protocols designed to protect sensitive data.

Lead City University Ibadan DO NOT COPY

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 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[9]. While the significance of employee involvement in information security is widely acknowledged, recent research shows that the topic is still not well understood. Many employees continue to demonstrate limited awareness of key security concerns, organizational policies, and proper procedures, which poses a challenge to effective implementation[9]. Raising employees' awareness and understanding of information security significantly reduces the chances of security breaches caused by human error or misconduct. It also strengthens the effectiveness of an institution's protective measures and response strategies, making overall security efforts more efficient and reliable[10]. Therefore, gaining insight into the elements that shape individuals' understanding of information security is essential. While recognizing these factors, organizations can better harness awareness to positively guide employee behavior and design more impactful security education programs.

This study presents a comprehensive review of existing literature on information security, aiming to identify and categorize the key factors that influence its effectiveness. While examining this specific area of research, the study offers valuable insights for both academics and practitioners, providing a structured overview of the fragmented knowledge in the field. It highlights inconsistencies, uncovers shortcomings, and points to areas that warrant further investigation. The findings are particularly beneficial for security managers in academic institutions, as they offer guidance on enhancing awareness programs, strengthening employee understanding of information security, and promoting better compliance with

Lead City University Ibadan DO NOT COPY

established policies. Ultimately, the quality of information security depends on how confidential data is handled, the accuracy and reliability of information, and its availability when needed[11].

Confidentiality in information security refers to the protection of sensitive data from being exposed to unauthorized individuals, such as competitors or media outlets. It ensures that access to information is restricted to those with proper clearance, preserving privacy and preventing potential misuse[11]. Confidentiality refers to the condition in which information is shielded from being accessed or revealed to individuals or systems without proper authorization. Breaches of confidentiality can occur in various ways, such as when an employee unintentionally exposes sensitive data or when a cybercriminal infiltrates an organization's database to steal client information. Integrity, on the other hand, ensures that data remains unaltered and trustworthy. It involves protecting information, like pricing details, email contacts, and other confidential institutional records from unauthorized changes. Integrity also signifies that the information is complete, accurate, and dependable, allowing users to rely on its authenticity and quality[11]. For instance, computer viruses and worms often compromise data integrity by damaging or altering files. Similarly, when unauthorized personnel modify information, they undermine its reliability. Availability, another key pillar of information security, refers to ensuring that authorized users can access the data they need when they need it. Disruptions such as denial-of-service (DoS) attacks can interfere with this access, making critical information temporarily invisible or unreachable. The confidentiality, integrity, and availability of institutional data are constantly exposed to various risks. Sensitive information might be leaked to competitors, students, or unauthorized staff. Data can be corrupted due to hardware failures or malicious cyber activity, and access may be

Lead City University Ibadan DO NOT COPY

hindered by network congestion or system outages. To effectively protect these core elements, it is essential to identify and understand the specific threats that institutions face[12].

Today's information security landscape faces a wide range of threats that can compromise the confidentiality, integrity, or availability of data. These threats are typically classified into three main categories: accidental or unintentional incidents, deliberate or intentional attacks, and contributory or instrumental factors that indirectly support or enable security breaches[13]. Accidental or unintentional threats arise from events beyond the control of IT systems, including natural disasters like floods or earthquakes, technical failures, and mistakes made by individuals. These incidents can disrupt operations and compromise the security of information without any malicious intent[14]. Intentional threats can range from harmless to harmful, depending on the motive behind them. Malicious threats, in particular, aim to damage, exploit, or compromise targeted information. These attacks often involve tactics such as deploying malware, executing hacks or system intrusions, launching denial-of-service (DoS) attacks, or engaging in theft, fraud, and espionage[14]. Benign threats often contribute to exploration to find flaws in a system or purposefully flaunting system flaws. Contributory or instrumental threats arise when proper procedures are either lacking or not effectively enforced. For example, allowing unrestricted access to IT systems poses a procedural risk. These threats may stem from weak or missing practices such as failing to perform regular backups, using poor password protocols, neglecting website access restrictions, permitting uncontrolled use of external storage devices, or overlooking email security guidelines.

Accidental threats stem from events outside human control, including natural catastrophes like earthquakes or floods, technical malfunctions, and mistakes made by individuals. These types of incidents can disrupt systems and compromise information security without any deliberate intent[15]. Natural disasters pose a significant threat to information security, and are

Lead City University Ibadan DO NOT COPY

often referred to as “environmental threats” in academic and professional discussions. These threats encompass a wide range of events, including fires, whether electrical or caused by wildfires flooding from rivers, heavy rainfall, or seawater intrusion, and structural damage or collapse due to earthquakes, vehicle collisions, or building failures. Other environmental risks include power outages that can disable or permanently damage IT systems and security infrastructure, making access to facilities or data impossible. Failures in computer or telecommunications systems may result in data loss or delays while backups are restored. Inadequate climate control, such as air conditioning breakdowns in server rooms, can lead to overheating and equipment failure. Human-related factors also contribute to environmental threats. These include incorrect data entry by staff, software bugs that produce inaccurate information, and the absence or illness of key IT personnel, which can impact system availability. Additionally, poor placement of IT facilities, such as being near areas prone to political unrest or labor disputes, can prevent staff from accessing critical infrastructure when needed[16].

Deliberate or intentional threats refer to actions specifically aimed at compromising or exploiting sensitive information, whether for harmful or strategic purposes. These threats often involve malicious techniques such as deploying malware, conducting system hacks or intrusions, launching denial-of-service (DoS) attacks, and engaging in theft, fraud, espionage, or even acts of arson targeting physical infrastructure[17]. Malware refers to software specifically created with harmful intent. It includes various forms such as viruses, Trojan horses, and spyware. Viruses, in particular, contain code designed to alter files and carry out unauthorized actions. They are intentionally distributed among users to infect systems, often spreading further and causing damage or data loss. While some viruses may produce minor effects, like displaying a message, others can seriously corrupt files or software. The development of new viruses is ongoing, and their impact can be substantial. Cybercriminals

Lead City University Ibadan DO NOT COPY

often design malicious tools like logic bombs, worms, and Trojans, all of which pose serious risks to data confidentiality[17].

Intrusions refer to any form of attack aimed at gaining unauthorized entry into a computer system or network. These breaches can be carried out through various techniques, all intended to bypass security measures and access sensitive data or resources without permission[18]. Denial of Service (DoS) attacks aim to disrupt normal access to digital systems by overwhelming them, making essential resources unavailable to authorized users. These attacks are designed to block legitimate activity, often by flooding networks or servers with excessive traffic that causes them to crash or become unresponsive[19]. Unauthorized attempts to access digital information often take the form of hacking or tapping. Hacking involves breaching a network without permission, while tapping refers to physically connecting to communication lines to intercept data. Although some hackers act to showcase their technical abilities, their actions can seriously compromise the confidentiality, integrity, and availability of information. One common tactic involves embedding malicious code into software that activates later, corrupting files or systems. For example, a disgruntled programmer might insert code that deletes a file if their name is removed from an internal database following termination.

Laptop theft also poses a major security risk. When a device is stolen, users may lose not only the hardware and software but also critical data that hasn't been backed up. Moreover, the thief could gain access to confidential files and personal information, further endangering privacy and organizational security[19]. To combat data theft, a variety of protective measures have been introduced, including security alarms, physical locks for laptops, and visual deterrents like warning stickers or identification labels. Fraud, defined as a deliberate attempt to unlawfully obtain someone else's property or money through deception or manipulation,

Lead City University Ibadan DO NOT COPY

poses a serious threat to information security. It occurs across multiple sectors, with financial and online fraud being particularly common. Internet fraud, in particular, has become a convenient tool for cybercriminals to extract money or sensitive data, often through tactics like phishing schemes. The most effective defense against online fraud is education, which is knowing how to recognize and avoid scams is key to staying protected[20].

Contributory threats arise when proper protocols are missing or poorly implemented. One example is when IT equipment is left accessible without restrictions, creating a procedural vulnerability that can expose systems to unauthorized use or interference[21]. Procedural threats emerge when established protocols are ignored or inadequately enforced. For instance, if proper verification steps are missing, unauthorized individuals may gain access to IT equipment or storage media. Weak access controls can also allow unapproved users to view or alter sensitive data. To mitigate such risks, it is essential to maintain strict oversight during the development and modification of systems, ensuring that only verified and accurate programs are deployed into live environments[22]. Information systems are vulnerable when personnel are unreliable or improperly managed. To mitigate this risk, organizations must implement strict hiring practices that place trustworthy individuals in sensitive roles. Additionally, clear exit protocols are essential to ensure that departing employees no longer retain access credentials or identification that could compromise security. Inadequate training also poses a significant threat, as staff lacking the necessary skills or awareness may unintentionally expose systems to risk or fail to respond effectively to potential threats[21]. When employees lack proper awareness or training, the risk to information security rises significantly. A deeper understanding of modern threats, such as scams, hacking attempts, cyberattacks, fraud, phishing schemes, and identity theft, paired with an appreciation for the sensitive data stored on devices like computers, smartphones, thumb drives, and PDAs, can greatly improve asset protection. Equipping staff with the knowledge and skills to identify

Lead City University Ibadan DO NOT COPY

and respond to both actual and potential security issues is essential for maintaining a secure organizational environment.

Security breaches can lead to a wide range of damaging outcomes. One major consequence is the loss of confidentiality, where unauthorized individuals gain access to sensitive data due to compromised access controls. Another is the loss of integrity, meaning the information stored or generated by the system may no longer be accurate or trustworthy. Additionally, breaches can result in reduced availability, where systems fail to operate when needed. In extreme cases, such as the destruction of a data center, this loss of availability can be permanent, severely disrupting organizational operations[23]. The impact of security breaches, whether isolated or combined, can be severe, affecting not just the information system but the entire organization. That's why it is essential to evaluate security threats within the broader corporate framework. The IT department plays a central role in organizational operations, and any disruption to its functions can ripple outward, potentially jeopardizing the organization's stability. For instance, a shift in management policies that negatively affects IT staff morale may increase the likelihood of mistakes or negligence. If such errors result in the loss of critical business data or cause significant delays, the consequences for the organization can be substantial[23]. Identifying and evaluating the key factors that lead to information security breaches is challenging due to the wide variation in organizational structures and technological requirements. What qualifies as adequate protection in one context may not be suitable in another, and these standards often shift as conditions evolve. To ensure effective security, organizations must consider the specific vulnerabilities and sensitivity of their systems and data, as well as the practicality and cost of implementing appropriate safeguards[24].

Lead City University Ibadan DO NOT COPY

Information risk refers to the likelihood that a specific action or incident could either hinder or support an organization's ability to meet its goals. It encompasses both potential threats and opportunities that arise from how information is managed, protected, or exposed[25]. Risk management is a continuous process designed to minimize the impact of adverse events. It involves identifying vulnerabilities within an organization's information systems and implementing measures to ensure that any potential losses remain within acceptable limits. This approach offers a structured method for addressing threats, supported by a wide range of strategies, techniques, and software tools. Each component of a system or project may face unique risks or interpret those risks differently, requiring tailored responses. The standard framework for managing risk typically includes the following steps: identifying potential hazards, evaluating their impact, developing appropriate safeguards, making informed decisions, applying the chosen controls, and continuously monitoring and reviewing the situation[25]. This pattern is reflected in a number of more formal models of the process.

Most risk management models follow a standard sequence of steps, some scholars propose additional elements to enhance the process. One such recommendation is the inclusion of an initial asset identification phase, which involves clearly defining the resources that need safeguarding, such as hardware, software systems, and personnel. This foundational step helps ensure that all critical assets are accounted for before assessing vulnerabilities and implementing protective measures[26]. An important phase in the risk management process involves selecting countermeasures that are both effective and economically viable, aiming to reduce risk to a level the organization considers acceptable. Once these safeguards are implemented, it is essential to reassess the risks to verify that the chosen measures are working as intended. Additionally, contingency planning plays a critical role in preparing for unforeseen disasters that may bypass existing protections. These plans support recovery

Lead City University Ibadan DO NOT COPY

efforts and help ensure continuity in the face of unexpected disruptions[26]. From this analysis of risk management frameworks, it can be concluded that, despite slight differences in terminology and occasional additions, the overall structure reflects widely accepted principles. As such, it serves as a practical and reliable model for managing information risk. The sections that follow will explore each stage of the process in detail.

The first step in identifying risks is to recognize all the components, assets, and resources that make up a computing system or are essential to its operation, as each of these may be vulnerable to threats. These elements span several categories. Hardware includes items such as central processors, disk drives, terminals, modems, shredders, and storage cabinets. Software encompasses operating systems, compilers, application programs, audit tools, security logs, and backup files. Data and media refer to master files, input and output data, software documentation, procedural manuals, disk packs, magnetic tapes, and data cards. Communication assets involve telephone circuits, postal services, private data carriers, and network infrastructure. Environmental factors include the physical building structure, power supply systems, air conditioning units, cleaning and catering services, and elevator access. Organizational elements cover management policies, internal structures, and personnel across IT, technical, administrative, and secretarial roles. Lastly, support services consist of maintenance teams, auditors, consultants, and delivery staff. Identifying these assets is a critical foundation for assessing vulnerabilities and implementing effective risk management strategies[26].

Once a comprehensive inventory of all vulnerable assets and resources has been compiled, each item should be evaluated against the various types of risk it may face, such as unintentional damage, intentional exposure, or unauthorized access. It is equally important to consider the potential sources of these risks, which may include natural disasters like fire or

Lead City University Ibadan DO NOT COPY

flooding, deliberate acts of sabotage, or disruptions caused by labor disputes. This step ensures that every component of the system is assessed in light of both the nature and origin of possible threats[26]. In evaluating potential risks, it is important to recognize that a single incident can simultaneously affect multiple components of a computing system. This is often due to the interconnected nature of system elements, where the occurrence of one risk may trigger or amplify others. Risks can be broadly categorized into several types. Property losses include physical damage, destruction, theft, loss, or contamination of assets. Liability losses arise from legal issues such as breaches of contract or copyright, as well as defamation through libel or slander. Personnel losses involve disruptions caused by death, illness, injury, strikes, resignations, or extended absences. Financial losses may result from unpaid debts or dishonest behavior by employees. Lastly, business interruption losses refer to delays in cash flow, increased operational costs, or penalties due to unmet obligations. Understanding these categories helps organizations assess the full scope of potential threats and prepare more effective responses[27].

Risk analysis involves assessing both the likelihood and potential impact of various threats. Its purpose is to minimize the chances of those risks occurring, understand the severity of their consequences, and determine the most effective strategies for managing each specific outcome[28]. Assessing and measuring risks, along with their potential consequences, is a key part of the risk analysis process. This can be done using a range of techniques, which may be either qualitative or quantitative. One widely used quantitative method involves calculating the expected loss, a monetary estimate that reflects the financial impact of a specific risk. This figure is typically derived by multiplying the average cost of a potential loss by the frequency with which that risk is anticipated to occur annually. While a yearly timeframe is commonly used for convenience, other intervals may be applied depending on the context. To

Lead City University Ibadan DO NOT COPY

effectively determine the severity of a risk and the necessity for countermeasures, two factors are especially important: the potential impact (or loss) and the likelihood of occurrence. These values should be based on the most accurate and informed estimates available. Once expected losses have been calculated for each identified risk, they should be ranked in descending order, allowing organizations to prioritize their response strategies based on the most significant threats[27].

In principle, the greater the estimated financial impact of a potential risk, the more critical it becomes to implement appropriate countermeasures. Prioritizing risks based on their expected loss ensures that the most serious threats are addressed first, helping to protect the organization from significant disruptions or damage[27]. When choosing countermeasures, it is essential to evaluate both their cost and their ability to reduce expected losses. The goal is to identify a combination of safeguards that, within the limits of available resources, minimizes the total of all anticipated losses and the expenses associated with implementing those measures. While financial constraints are a major consideration, other critical risks, such as the disruption of essential real-time operations or the exposure of confidential information, must also be prioritized due to their potential to threaten the organization's survival. Once risks have been identified, their likelihood assessed, and their potential impact understood, the focus must shift to determining how best to respond. This involves selecting specific strategies to address individual threats and preparing contingency plans for unforeseen events. It is equally important to establish clear procedures for deploying these measures, as well as systems for monitoring, reviewing, and updating them to ensure ongoing effectiveness.

There are four fundamental strategies for managing risk, one of which is avoidance. This approach involves eliminating the possibility of a particular risk altogether, often by choosing not to implement a specific system, facility, or piece of equipment that could introduce

Lead City University Ibadan DO NOT COPY

vulnerabilities. In some cases, modifying operational procedures or workflows can also help sidestep potential threats before they arise[28]. Choosing to avoid a particular risk may be a deliberate decision or a necessity when implementing effective countermeasures proves too complex or costly. Regardless of the reason, it is essential to remain alert to any internal or external changes that could reintroduce the risk. Another approach is risk retention, where an organization consciously decides not to take direct action against a threat deemed to have minimal impact, one that can be managed without causing significant disruption or embarrassment. In such cases, the organization accepts full responsibility for any consequences that may arise from the risk[28]. Organizations may choose to retain risks that are inexpensive yet occur frequently, as these are often manageable without significant disruption. However, retaining risks that are rare but potentially costly can be extremely dangerous and may lead to serious consequences. It is essential to continuously monitor for changes in internal or external conditions that could elevate the severity of retained risks. Importantly, deliberate risk retention must be clearly distinguished from accidental oversight, failing to identify a risk altogether can result in unexpected and potentially embarrassing outcomes.

Reduction refers to the strategy of minimizing the impact of potential risks through the use of preventive measures. For instance, implementing access control systems can significantly lower the likelihood of unauthorized individuals entering sensitive areas like computer rooms. While these countermeasures can be highly effective, they often come with additional financial costs that must be weighed against the benefits they provide[28]. While some countermeasures may involve added costs, others can be implemented through procedural adjustments, making them more cost-effective. Another strategy is risk transfer, which involves shifting the responsibility for certain risks to external parties. This can be achieved through contingency planning, insurance policies, or contractual agreements. Although

Lead City University Ibadan DO NOT COPY

preventive measures can help reduce how often risks occur and lessen their impact, it is important to recognize that not all risks can be completely eliminated[28]. When risks do materialize, having a well-developed contingency plan can help ensure that critical systems continue to function, minimizing disruption. Insurance can also offer financial compensation for losses incurred, but it is not always the most cost-effective solution. Although premiums are predictable, many policies include excess clauses that exclude coverage for the initial portion of a claim. This means that part of the risk remains with the insured, effectively becoming a retained risk. Another way to transfer risk is through contractual arrangements, such as warranties or maintenance agreements. However, it is essential that any third party assuming the risk, whether an insurer or contractor, is trustworthy and financially stable. It is important to note that not all risks can be transferred, and insurance should never be viewed as a replacement for robust preventive measures.

In the field of information security, skilled personnel and advanced technologies play a vital role in minimizing and managing risks. One common vulnerability is the use of weak or easily guessable passwords, which can be exploited by hackers using a variety of techniques, including social engineering. Passwords that are short, simplistic, or contain personal details like names or birthdates are particularly susceptible to being cracked, making systems more vulnerable to unauthorized access and potential data breaches[29]. Passwords that are long and complex, typically exceeding eight characters and incorporating a mix of numbers, uppercase and lowercase letters, and special symbols, are significantly harder for attackers to crack, offering stronger protection against unauthorized access and data theft. However, relying solely on a strong password is not sufficient for complete security. Regularly updating passwords helps limit the risk of exposure over time. In addition to sound password practices, robust internet security tools play a vital role in safeguarding information. Software such as

Lead City University Ibadan DO NOT COPY

antivirus programs, anti-spyware, anti-spam filters, and firewalls can help preserve user privacy and defend against a wide range of threats, including malware, Trojans, spyware, and hacking attempts[29]. In the field of information security, many risks stem from user negligence or a lack of understanding about the importance of safeguarding data. When individuals fail to recognize the value of the information they handle, they may unintentionally expose systems to threats. However, with proper training and heightened awareness, users can play a crucial role in preventing and mitigating these risks. It is essential that all personnel are familiar with the organization's security policies and standards, as this knowledge empowers them to protect sensitive information and maintain the integrity of the system.

Once the technical aspects of risk management have been addressed, the next crucial step is to establish and enforce a comprehensive information security policy. Since the 1970s, significant advancements have been made in how these policies are defined and implemented. Today, information security policies serve as the cornerstone for protecting an organization's digital assets and resources. As technological threats continue to evolve, institutions are increasingly refining and updating their policies to meet emerging challenges and ensure robust protection across all levels of operation[29]. An effective information security policy must integrate physical, technical, and non-technical components to ensure long-term compliance and resilience. This holistic approach helps safeguard systems not only through hardware and software protections, but also through procedural standards, user awareness, and organizational practices[29]. Information security policies are formal declarations that outline how an organization identifies, evaluates, and manages risks stemming from its operational activities. These policies guide decision-making by weighing the cost of mitigating risks against the potential benefits to the organization's mission. A well-structured policy document should clearly articulate the organization's security principles, outline the

Lead City University Ibadan DO NOT COPY

procedures and requirements for maintaining protection, and define both general and role-specific responsibilities related to information security.

Technology serves as a powerful catalyst for global integration and collaboration, offering individuals expanded opportunities for interaction and exchange. Yet, its dual nature also introduces significant vulnerabilities. As technology evolves, its alignment with local cultural and environmental contexts is frequently scrutinized through empirical testing and theoretical evaluation. One critical cultural dimension, interpersonal skills, is often examined within the framework of Hofstede's cultural model, which identifies variables such as individualism and collectivism. These cultural traits profoundly influence how information security practices are shaped and executed. The diversity of user backgrounds and the inherent vulnerabilities of technological systems underscore the importance of understanding cultural responses to security protocols. Hofstede's Framework provides a valuable lens for analyzing how cultural differences among users affect their engagement with technology and their perception of security measures[30].

Hofstede's cultural dimensions are evaluated through the lens of societal values and national backgrounds. In his analysis, Malaysia serves as a case study where the structure of information systems is notably shaped by hierarchical norms. The Hofstede Framework seeks to understand how different cultures interact with information technology, including their expectations, operational behaviors, and readiness for adoption. One key dimension, Uncertainty Avoidance, plays a significant role in shaping how organizations manage technological systems. Within this context, Enterprise Resource Planning (ERP) systems are highlighted as critical components for ensuring operational stability and consistency, particularly in environments where minimizing uncertainty is a cultural priority[30].

Lead City University Ibadan DO NOT COPY

Hofstede's cultural framework has not yet achieved universal acceptance in terms of its validity and alignment with localized information security systems. Nonetheless, it continues to find relevance across various societal domains, particularly in relation to modern technological tools. Hofstede sought to explore how cultural dimensions interact with technological variables, examining the reciprocal influence between societal values and the adoption or operation of digital systems. The foundation of his research traces back to his tenure at IBM, where he conducted one of his seminal studies on cultural differences and their impact on organizational behavior and technological engagement[30]. Each of Hofstede's cultural dimensions offers valuable insight into how his framework can be applied to the domain of information system security. One particularly relevant dimension is Long-Term Orientation (LTO), which aligns closely with the evolving nature of technology and the sustained commitment required to maintain robust security measures over time. This perspective emphasizes the importance of forward-thinking strategies in both technological advancement and cybersecurity planning.

Conversely, the Masculinity dimension holds limited relevance in the context of information security, as the sensitivity and critical nature of data protection transcend gender roles and user types. Security protocols must be universally applicable, regardless of cultural associations with competitiveness or assertiveness. A frequently overlooked yet crucial aspect of information security is the role of data handling policies. These policies govern how information is stored, accessed, and shared, directly influencing the integrity and confidentiality of digital systems. Integrating cultural awareness with sound data governance can significantly enhance the effectiveness of security frameworks.

2.1.2 Concept of Data Handling Stages

Lead City University Ibadan DO NOT COPY

Data handling stages outline 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[31]. 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. When applied specifically to academic data, this policy reflects the increasing importance of privacy in line with evolving regulatory standards. It provides clear, actionable guidelines for responsibly managing personally identifiable information, ensuring that institutions meet both legal and ethical obligations. While aligning with stringent privacy laws, such policies help organizations avoid financial penalties and reputational damage, making them indispensable in today's compliance-driven environment.

Data handling stages outline the principles and procedures an 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. Ultimately, it serves as a roadmap for safeguarding sensitive information and maintaining public trust[32]. A well- designed data handling stages strengthens information accountability by ensuring that organizations respect individuals' rights and maintain public trust in their data practices. At its core, the policy establishes procedures for classifying data according to its sensitivity and defining the appropriate methods for handling, storing, and transmitting each category. Data classification is a critical element, as it aligns

Lead City University Ibadan DO NOT COPY

security measures with the sensitivity level of the information, allowing resources to be focused on protecting the most valuable and vulnerable assets.

This targeted approach supports practical application by enabling efficient risk management, ensuring that highly sensitive data receives robust protection while minimizing unnecessary exposure. Beyond security, a data handling stages provides a structured framework for managing information effectively, with clear guidelines for organizing, storing, and retrieving data. It promotes both operational efficiency and strong safeguards, ensuring that information remains accessible to authorized users while being protected against misuse. In doing so, it strikes a careful balance between meeting organizational needs and upholding rigorous protective measures.

Data handling policies are a foundational element of modern organizational data governance, providing a structured framework for managing information throughout its entire lifecycle. They set out clear, organization-wide standards for the collection, processing, storage, transmission, and eventual disposal of data. In doing so, they not only safeguard sensitive data but also reinforce accountability, transparency, and trust in the organization's data management practices[33]. The importance of clearly defined data handling policies has increased dramatically in response to the growing complexity of modern data ecosystems and the introduction of stricter global privacy regulations. At the heart of these policies lies data classification, which serves as the essential first step in ensuring effective information governance. Organizations must develop precise criteria for categorizing data according to its sensitivity, applicable legal requirements, and overall business value. A robust classification framework typically includes categories such as public, internal-use, confidential, and highly restricted data. Each classification level demands tailored handling procedures, access controls, and security measures that correspond to the sensitivity and criticality of the

Lead City University Ibadan DO NOT COPY

information. This structured approach ensures that protection efforts are proportionate, resources are allocated efficiently, and the most valuable or vulnerable data receives the highest level of safeguarding.

The importance of clearly defined data handling policies has increased dramatically in response to the growing complexity of modern data ecosystems and the introduction of stricter global privacy regulations. At the heart of these policies lies data classification, which serves as the essential first step in ensuring effective information governance. Organizations must develop precise criteria for categorizing data according to its sensitivity, applicable legal requirements, and overall business value. A robust classification framework typically includes categories such as public, internal-use, confidential, and highly restricted data. Each classification level demands tailored handling procedures, access controls, and security measures that correspond to the sensitivity and criticality of the information. This structured approach ensures that protection efforts are proportionate, resources are allocated efficiently, and the most valuable or vulnerable data receives the highest level of safeguarding[33]. Modern access control frameworks increasingly embrace the principle of least privilege, granting users only the minimum level of access required to perform their duties. This approach reduces the risk of unauthorized data exposure and limits the potential impact of security breaches. Effective policies also define clear authentication standards, outlining how users verify their identities; authorization procedures, specifying the conditions under which access is granted or modified; and regular access reviews to ensure permissions remain appropriate over time. Together, these measures create a dynamic and adaptive security posture that safeguards sensitive information while supporting operational efficiency.

Data handling policies must be designed to comply with applicable regulatory frameworks and recognized industry standards. The General Data Protection Regulation (GDPR) sets out

Lead City University Ibadan DO NOT COPY

comprehensive rules for managing the personal data of European Union residents, shaping data governance practices worldwide. In the United States, laws such as the California Consumer Privacy Act (CCPA), along with other state-level regulations, establish specific requirements for data processing and consumer privacy rights. Additionally, sector-specific standards impose further obligations, such as the Health Insurance Portability and Accountability Act (HIPAA), which governs the protection of healthcare information, and the Payment Card Industry Data Security Standard (PCI DSS), which outlines strict controls for safeguarding payment card data. Together, these regulations form a complex compliance landscape that organizations must navigate to ensure lawful, ethical, and secure data management[33]. Organizations must ensure their policies address these specific regulatory requirements while maintaining operational efficiency.

The expansion of remote work has created significant new considerations for data handling policies. Organizations must account for the heightened security risks associated with accessing sensitive information from diverse locations, networks, and devices. This requires implementing safeguards that protect data integrity and confidentiality while ensuring continued compliance with applicable regulatory requirements. Policies should address secure connection protocols, device management standards, and user authentication measures, as well as provide clear guidance for employees on safe data practices outside traditional office environments[34]. Effective data handling policies for modern institutions must incorporate robust technical safeguards, including strong encryption protocols, secure authentication measures, and continuous monitoring systems to protect data accessed remotely. The growing reliance on cloud computing and third-party service providers introduces additional layers of complexity, requiring clearly defined standards for

Lead City University Ibadan DO NOT COPY

cloud-based data storage and processing. These should include mandatory encryption, regular backup schedules, and comprehensive disaster recovery plans to ensure resilience.

Equally important is vendor management, which demands thorough due diligence before engaging service providers, as well as contractual clauses that clearly define data protection responsibilities and compliance obligations. In today's regulatory climate, data privacy has become a central pillar of handling policies. Academic institutions, in particular, must implement transparent procedures for obtaining and managing user consent, responding to data subject requests, and openly communicating how personal information is processed. This approach not only ensures compliance with privacy laws but also strengthens trust between institutions and their stakeholders[34]. Privacy impact assessments have become standard components of data handling policies, helping organizations identify and address potential privacy risks before implementing new data processing activities.

Institutions generate records to document and support their operations. However, without proper management, these records may fail to serve their intended purpose, leading to the loss of critical information and potential operational challenges. To maintain an efficient and effective administration that ensures smooth business processes, records must be systematically organized and safeguarded. In the context of academic institutions, data handling refers to the application of structured, scientific, and controlled methods for managing recorded information throughout its lifecycle. This ensures that essential data remains accurate, accessible, and secure, thereby supporting institutional goals and compliance requirements[35]. Data handling is a specialized area of management focused on the efficient and systematic oversight of data throughout its lifecycle. This includes the creation, receipt, maintenance, utilization, and final disposition of information, as well as the processes for capturing and preserving evidence of academic activities and institutional transactions. It

Lead City University Ibadan DO NOT COPY

also encompasses the disciplined application of established methods and procedures to manage information generated internally as a result of an institution's own operations. While maintaining structured control over these processes, organizations ensure the integrity, accessibility, and reliability of their data assets.

Furthermore, data handling refers to the structured and methodical management of all forms of data, whether in digital media or printed format, from the point of creation through to its final disposition. This process encompasses the formulation and application of standards that govern every stage of the data lifecycle, including its creation, utilization, storage, retrieval, disposal, and long-term archival preservation[36]. An effective data handling stages ensures that information is readily available when required, that privacy and confidentiality are preserved, and that redundant or obsolete data is securely destroyed. Ultimately, such a policy supports the continuity and quality of service delivery. Over time, the term data handling has increasingly been used interchangeably with information management, reflecting the minimal distinction between the two. While information management encompasses the oversight of all institutional information, along with the people, hardware, software, and systems involved in its creation, data handling can be viewed as a core component of this broader discipline[36].

Information management is an overarching discipline within which data handling operates as a specialized function. The primary purpose of data handling is to manage and regulate the flow of data and the associated information within an institution. It involves the systematic control of recorded data essential for carrying out institutional activities. This function spans the entire data lifecycle, from creation or receipt, through processing, distribution, and institutional use, to storage, retrieval, and eventual disposal.

Data handling stages formalizes this process by setting out the standards and procedures for managing any information captured in reproducible form that is necessary for academic and

Lead City University Ibadan DO NOT COPY

administrative operations. 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[36]. Data handling stages is concerned with the generation, receipt, processing, storage, distribution, use and disposal of records[36]. Data handling spans a broad range of activities and sub-disciplines, including the management of mail, correspondence, reports, copies, forms, and directives. It is fundamentally the process of exercising control over institutional information from its creation to its final disposition. This involves the systematic management of data throughout its lifecycle, from the moment it is generated or received, through its processing, distribution, and placement within storage and retrieval systems, to its eventual secure disposal or designation for permanent archival preservation. In essence, data handling represents the professional stewardship of recorded information, ensuring that it remains organized, accessible, and protected in alignment with institutional, legal, and operational requirements[36].

Institutions generate data to support the functions and activities they perform. However, without proper management, this data may fail to provide the necessary support, leading to the loss of valuable information and operational challenges. To ensure smooth, efficient, and effective administration, data must be systematically managed throughout its lifecycle. It is now widely acknowledged that improvements in the delivery of administrative services, particularly by Non-Academic Staff, are closely tied to effective data handling. Strong data management practices enhance information exchange, enable evidence-based policy formulation, uphold data protection principles, promote accountability, and strengthen decision-making and knowledge management across all sectors of government[37]. Effective data handling can play a pivotal role in advancing the achievement of the United Nations Millennium Development Goals (UNMDGs). Access to complete, accurate, and timely data

Lead City University Ibadan DO NOT COPY

is essential for tracking progress, identifying gaps, and formulating targeted interventions. Well-managed data underpins sound decision-making, enabling policymakers and institutions to design strategies that address pressing social, economic, and environmental challenges.

Furthermore, data is a critical resource for driving development in any nation. The core pillars of sustainable progress, such as good governance, an equitable judicial system, a transparent and accountable financial sector, and the protection of enforceable civil rights, are all underpinned by robust data and information management infrastructures. Without accurate, accessible, and well-managed data, these foundational elements cannot function effectively, as informed decision-making, policy formulation, and accountability mechanisms all rely on the integrity and availability of reliable information[38]. Without a robust data infrastructure, academic institutions may struggle to manage their current operations effectively and lose the capacity to draw on past experiences for strategic guidance. Data serves as a critical asset for the efficient and productive functioning of organizations, providing the factual foundation upon which decisions are made. In academic settings, such as polytechnics, data captures and documents institutional decisions, activities, and outcomes. These records act as benchmarks, enabling institutions to evaluate performance, measure progress, and inform future actions with evidence-based insights[38].

Without reliable data, the foundations of the rule of law and accountability are severely weakened, making effective administration impossible. In the absence of accurate and well-managed information, officials are often compelled to make decisions on an ad hoc basis, lacking the benefit of institutional memory or historical reference. Furthermore, without proper data, fraudulent activities cannot be substantiated, meaningful audits cannot be conducted, and administrative actions remain beyond effective review. Robust data

Lead City University Ibadan DO NOT COPY

management is therefore essential for transparency, oversight, and the integrity of governance processes[38]. Data is recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprise content, context and structure sufficient to provide evidence of the activity, and support informed decision making.

Data refers to recorded information, regardless of its form or medium that is created, received, and maintained by an institution or individual in fulfilling legal obligations or conducting business activities. Such data serves as evidence of the performance of those obligations or transactions. This definition extends beyond traditional paper-based records like correspondence, reports, and forms, encompassing all formats that capture valuable information.

As a critical business asset, data holds significant value for institutional operations and decision-making. A systematic approach to its management is essential for both institutions and society, ensuring that data is protected, preserved, and maintained as reliable evidence of actions taken. Within academic environments, an effective data handling system provides a dependable source of information on both academic and administrative activities. This, in turn, supports future initiatives, informs academic decision-making, and upholds accountability to current and future stakeholders[38].

Data constitutes a distinct category of information, characterized by its evidentiary value and capacity for legal verification. The effective creation and preservation of such data depend on systematic control throughout its lifecycle. This lifecycle can be summarized as the structured process of managing data from its initial creation to its ultimate disposition, encompassing its generation, control, maintenance, utilization, and secure disposal. An effective data handling stages ensures that personnel data is managed consistently and in a well- structured manner across all stages of its existence. Such a policy enables institutions to fulfill their legal and

Lead City University Ibadan DO NOT COPY

regulatory obligations, facilitates timely access to information for policy formulation and planning, safeguards the integrity and accuracy of data, and ensures that it can be readily retrieved when required[39]. This brings us to the discussion to data handling stages. Data handling stages has been defined in various ways, but all definitions share common elements. At its core, it is the systematic practice of identifying, classifying, collecting, preserving, and ultimately disposing of recorded data in an organized manner. It involves managing data throughout its entire lifecycle, from creation and receipt to maintenance, use, and final disposal, while applying structured and scientific controls to the information required for an organization's operations. As a specialized field of management, data handling ensures the efficient and consistent oversight of data processes, including the capture and preservation of evidence of academic activities and institutional transactions. Regardless of the definition used, the common denominators remain clear: systematic control of data at every stage, preservation of its evidentiary value, alignment with operational and legal requirements, and the maintenance of integrity, accessibility, and security through structured processes[39]. These are reliability, integrity, compliance, comprehensiveness, and that it must be systematic.

Data handling stages governs not only the broader activities of data management but also the conduct of every individual who creates, accesses, or uses data in the course of their duties. Within an institution, such a policy encompasses the establishment of clear policies and standards, the assignment of responsibilities and authority, and the development and dissemination of procedures and guidelines. It also involves delivering a range of services related to the management and use of data, as well as designing, implementing, and administering specialized systems for data governance. Furthermore, an effective data handling stages ensures that data management practices are fully integrated into the institution's administrative systems and processes, creating a cohesive framework that

Lead City University Ibadan DO NOT COPY

supports operational efficiency, compliance, and accountability[39]. Data handling stages incorporates the policies, systems and professional and management techniques, systematically applied to the control of recorded information to enhance an organization's efficiency and effectiveness, while at the same time consolidating its evidential base. While data handling and records management share similarities, there are important distinctions between the two. Records management is a professional discipline primarily concerned with the oversight of document-based information systems, most of which exist in paper format. Data handling, by contrast, is more commonly associated with database information systems in digital environments, where information is stored and managed electronically.

To understand this distinction, it is useful to consider the broader concept of information, defined as any form of intelligence that can be communicated, whether in graphic form or through alphanumeric characters. This definition encompasses the entire spectrum of data, documents, and files created and maintained by institutions. In this context, data handling refers to the administration of information, its use, transmission, and the application of information science principles and techniques to design, enhance, or optimize systems for managing data effectively[40]. The primary objectives of data and records management are to provide accurate, timely, and complete information that supports effective decision-making in the management and operation of an organization. This involves processing data and records as efficiently as possible, delivering information at the lowest feasible cost, offering maximum service to data users, and securely disposing of records that are no longer required.

Data follows a defined lifecycle, beginning at the point of creation or receipt by an institution, continuing through its use and maintenance, and concluding with its final disposal. This lifecycle forms the foundation of a data handling stages, which outlines the specific procedures and processes to be applied at each stage. By ensuring that data is managed

Lead City University Ibadan DO NOT COPY

systematically from creation to disposal, institutions can maintain its integrity, accessibility, and relevance. Efficient lifecycle management is therefore a central principle of data management, enabling organizations to optimize resources, meet compliance obligations, and support informed decision- making.[40]. If institutional bodies do not control data through the earlier stages of their life-cycle, data that have low administrative value are kept too long and those of archival value cannot be identified and safeguarded[40]. All data passes through a defined lifecycle, beginning with its creation or receipt, the "birth" stage, followed by a period of active use, representing its "youth." As the data ages, it may transition into a "middle- aged" phase, where it is no longer in constant use but is still occasionally referenced. Eventually, it reaches its final stage, which involves either secure and confidential disposal or permanent preservation in an archive. Understanding this lifecycle is essential for designing effective data handling policies, as it ensures that appropriate controls, storage methods, and access provisions are applied at each stage to maintain integrity, security, and compliance.[40].

One of the fundamental principles underpinning a data handling stages is the concept of the data lifecycle. This concept forms the foundation upon which most data handling activities are built, as it provides a structured framework for understanding the various stages in the existence of data. The lifecycle outlines the progression of data from its initial creation or receipt, through its active use and ongoing maintenance, and ultimately to its final stage, whether that be secure disposal or permanent archival preservation[40]. The data lifecycle may extend beyond its period of active use, with information stored for an additional phase of infrequent or dormant access, often in secure off-site data centres. This stage concludes when the data's operational relevance ends entirely. At that point, it is either formally appraised or designated as archivally valuable, resulting in its transfer to a permanent archive, or deemed non- archival and securely destroyed. This final step ensures that data is either preserved as

Lead City University Ibadan DO NOT COPY

part of the institution's historical record or eliminated in a manner that protects confidentiality and complies with legal and regulatory requirements.

For sound data handling stages to be effectively implemented, institutional leadership must designate or appoint a senior-level staff member, often from the registry, who will be responsible for overseeing its execution and ongoing maintenance. This delegated officer should have the authority and resources necessary to ensure compliance with established standards and best practices. The Non-Academic Staff, in turn, should take the lead in developing a comprehensive data handling stages, ensuring it aligns with institutional objectives, legal requirements, and operational needs. Once formulated, the policy should be formally reviewed, endorsed, and supported by the head of the institution and the top management team, thereby reinforcing its authority and ensuring organization-wide adherence[41]. Adherence to data handling policies should be subject to continuous monitoring and formal review on an annual basis to ensure ongoing relevance and compliance. Institutions should maintain a clearly defined data handling stages to guide employees, supported by a robust data classification system that enables efficient retrieval, secure disposal, and proper retention of information. Regular training for registry and records office staff is essential to equip them with the skills required to perform their duties effectively. The loss or misplacement of critical information can have serious consequences, including jeopardizing the future of students who may require access to essential records. Registry and Archives staff should take responsibility for delivering appropriate data handling training programs to administrative personnel. Additionally, no data should be removed from the institution without the explicit authorization of the Non-Academic Staff, Archivist, or an appropriate Office Manager.

Lead City University Ibadan DO NOT COPY

Filing systems may be organized either centrally or departmentally, depending on institutional needs. In a centralized filing system, all institutional files are stored and managed in a single location, often overseen by a dedicated central filing department staffed by trained registry personnel. This approach promotes efficiency, ensures consistent filing practices, and allows for effective supervision of file movement and correspondence placement. In contrast, a decentralized or departmental filing system allows each department or section to maintain its own filing arrangements tailored to its specific operational requirements. Some organizations adopt a hybrid approach, combining elements of both systems to balance efficiency with departmental autonomy[41].

Over time, data handling stages has 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. Today, it encompasses the entire data lifecycle, from creation to final disposal, including periods of active use where data serves as a vital source of information. This process also involves systematic review against established retention schedules to determine whether data should be securely destroyed or preserved for long-term archival purposes. The modern approach reflects a shift from simple document storage to strategic information governance, ensuring that data remains accurate, accessible, and compliant with institutional, legal, and operational requirements throughout its existence[41]. The advent of computers has significantly enhanced the efficiency and value of data handling within institutions. For Polytechnics, data represents one of their most critical assets, underpinning decision-making, demonstrating regulatory compliance, documenting institutional history, and, most importantly, enabling the effective execution of core functions. To maximize the value of this asset while minimizing associated costs, data must be managed systematically and strategically.

Lead City University Ibadan DO NOT COPY

Well-implemented data handling stages allows institutions to control, reduce, and even eliminate unnecessary expenses related to data maintenance, while improving the efficiency of administrative operations. In today's interconnected digital environment, where Polytechnics may operate across multiple locations yet remain linked through the internet, centralized, standardized, and secure data management is not just logical but essential. Indeed, the importance of such policies has grown to the point where they are now considered a standard requirement in institutional administration, rather than an optional practice. In this era where institutions face mounting pressure to operate more efficiently while maintaining or enhancing service quality, data has emerged as a critical enabler of efficiency, accuracy, and accessibility of information. There is a clear link between strategic investment in data management and measurable productivity gains, including improved administrative services, faster response times, and enhanced service delivery.

The adoption of a 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. Importantly, such policies also enhance students' access to their academic records, thereby improving transparency, service quality, and institutional accountability[42].

While advances in information technology have brought significant benefits to academic institutions, they have also introduced a range of challenges that can hinder effective data management. Common issues include the absence of institutional plans for managing data, limited awareness of the role of data handling policies in promoting efficiency and

Lead City University Ibadan DO NOT COPY

accountability, and a lack of clear stewardship or coordination in managing both paper and electronic records. Other challenges involve the absence of enabling legislation, the lack of formal policies and procedures to guide data handling, insufficient core competencies in data management, and the absence of dedicated budgets to support these functions. Weak security and confidentiality controls, the lack of records retention and disposal policies, and the absence of strategies for migrating data to newer systems further compound these difficulties.

Despite these challenges, well-managed data has the potential to significantly enhance efficiency and productivity within the academic environment, particularly by improving the quality and speed of interactions between management and students. Addressing these gaps through comprehensive policies, skilled personnel, and adequate resources is therefore essential for institutions seeking to fully realize the benefits of modern information technologies[42]. Consequently, the use of certain technologies in data handling does not necessarily "free up time" for employees to engage in face-to-face interactions with colleagues. On the contrary, it can lead to a reduction in job satisfaction, as a greater proportion of working hours is spent in front of a computer. This shift in work patterns may limit opportunities for interpersonal collaboration, diminish workplace social engagement, and potentially affect overall staff morale.

One of the foremost challenges associated with implementing an effective data handling stages is the presence of weak legislative and institutional infrastructures. In many contexts, there is either no comprehensive legal framework governing data management or the existing laws are outdated, fragmented, or poorly enforced. This lack of robust legislation creates uncertainty around compliance requirements, data protection standards, and accountability measures. Similarly, institutional infrastructures may be underdeveloped, with inadequate organizational structures, insufficiently defined roles and responsibilities, and a lack of

Lead City University Ibadan DO NOT COPY

dedicated resources to support data governance. Without strong legal backing and well-established institutional mechanisms, policies often remain theoretical rather than operational, leaving data vulnerable to mismanagement, breaches, and loss of evidentiary value[43].

In many African academic institutions, data handling staff, particularly registry personnel, often lack the essential skills and competencies required for effective management of data and archives. A significant challenge is the prevalence of technophobia in many offices, especially among older employees. Limited proficiency in information technology has led many traditional librarians, Non-Academic Staff, and archivists to adopt a conservative approach, with some developing an aversion to computers[43]. This reluctance is partly rooted in a generational divide between older, analogue-trained professionals and younger, digitally adept staff. For some veteran information managers, the rise of computer-based systems is perceived as a threat to their long-established expertise and professional identity. In contrast, younger data managers tend to adapt more quickly to the use of ICTs, while older counterparts often struggle to meet the demands of the digital era. This skills gap poses a barrier to the modernization and efficiency of data handling practices in academic environments[43]. In many academic institutions, older data managers often display a strong reluctance to abandon long-established practices in favor of newer, technology-driven approaches. This resistance can hinder the modernization of data management processes and slow the adoption of more efficient systems. The successful implementation of data handling stages technologies therefore, depends not only on technical capacity but also on the ability to address and overcome both staff and personal resistance to change. Achieving this requires targeted change-management strategies, continuous training, and clear communication of the

Lead City University Ibadan, DO NOT COPY

benefits that modern systems bring to institutional efficiency, compliance, and service delivery[43].

The growing use of information technologies in the implementation of data handling policies has introduced significant challenges to the management of data in academic institutions. Across Africa and many developing countries, there is a strong drive to computerize core institutional functions, with governments encouraging or mandating the adoption of ICTs in the education sector. However, many of these initiatives fail to achieve their intended outcomes. A key reason for this is the lack of a thorough assessment of the existing information infrastructure to determine its suitability for supporting effective data handling policies. In addition, governments and implementing agencies often overlook the importance of consulting records managers, professionals whose expertise is essential in ensuring that automation processes preserve the reliability, authenticity, and evidentiary value of institutional records.

Without this critical input, automation efforts risk undermining the very functions they are meant to enhance, leading to systems that are technologically advanced but operationally ineffective in supporting accountability, compliance, and institutional memory[43]. The conversion from traditional records management activities to electronic environment will not succeed in Africa if the underlying processes are not structured in an efficient and effective fashion. Many African states are jumping into the information technology bandwagon without adequately incorporating a good data handling stages. The challenges associated with data handling stages in most organizations to corruption or inadequate finance. Corrupt leaders in Africa do not provide adequate funds, facilities, and infrastructure for proper and efficient data handling policies in academic institutions. Instead, corrupt bureaucrats intentionally distort the policies, decision-making apparatuses, and sometimes go to a lengths

Lead City University Ibadan DO NOT COPY

to transfer experienced records managers/Non-Academic Staff in a bid to create opportunities for embezzlement

The transition from traditional records 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.

A significant barrier to progress lies in the twin challenges of corruption and inadequate funding. In some contexts, leaders fail to allocate sufficient resources, facilities, and infrastructure to support proper and efficient data handling in academic institutions. More troublingly, corrupt bureaucrats may deliberately manipulate policies, disrupt decision-making processes, or even reassign experienced records managers and Non-Academic Staff to less critical roles, actions often intended to create opportunities for misappropriation of funds. Such practices not only weaken institutional capacity but also erode accountability, transparency, and trust in the management of academic records.

Lead City University Ibadan DO NOT COPY

2.1.3 Concept of Access Control

Access control is the process of granting or denying specific requests to access and use a resource or service. It functions as a decision-making mechanism, evaluating each request against established policies and rules through rules definition, permission allocation control, session management and user assignment control. A core principle it enforces is the principle of least privilege, ensuring that individuals are granted only the minimum level of access necessary to perform their specific roles or tasks. This approach not only protects sensitive

information but also reduces the risk of unauthorized use or security breaches[44]. Access control provides a structured approach to authorization, reducing the risk of unauthorized access by systematically managing permissions. Through this process, organizations can mitigate security threats and maintain a controlled environment. It is a core security technique that determines who or what can view, use, or interact with resources, and it applies to both physical and digital environments. While enforcing the principle of least privilege, access control ensures that only authorized entities, whether individuals, groups, or machines, are granted the minimum level of access necessary to perform their roles. This selective restriction of access emphasizes that entry to places, systems, or data should be limited to approved personnel, safeguarding protected assets and maintaining the integrity, confidentiality, and availability of resources across networks and computing systems[45].

Access control extends beyond individual users to include groups and machines, reflecting the complexity and interconnected nature of modern IT environments. It is the process of mediating every request to access resources and data maintained by a system, evaluating each request against predefined policies, and determining whether it should be granted or denied. Access control is one of the most fundamental pillars of information security, functioning as the primary mechanism for safeguarding resources and ensuring that only authorized access is granted within computer systems and organizational environments. While regulating who or what can interact with protected assets, access control upholds the confidentiality, integrity, and availability of information. It operates as a gatekeeping process, systematically evaluating each access request against established policies and permissions, thereby preventing unauthorized use and reducing the risk of security breaches[46].

The concept of access control has evolved considerably, progressing from simple permission systems to sophisticated, adaptive frameworks capable of meeting the complex and dynamic

Lead City University Ibadan DO NOT COPY

security requirements of modern computing environments. When implemented effectively, access control mechanisms enable organizations to maintain the confidentiality and integrity of their resources while ensuring their availability to legitimate users[47]. At its core, access control functions through the interaction between subjects, entities requesting access, such as users, devices, or processes, and objects, which are the resources being protected, including files, databases, applications, or system capabilities. This interaction is governed by comprehensive policies that define the precise conditions under which access should be granted or denied. The effectiveness of these policies depends on their alignment with both organizational security requirements and operational needs. The authentication process serves as the critical first step in access control, verifying the identity of subjects before they can request access to protected resources.

Modern authentication has advanced far beyond traditional password-based methods, now incorporating sophisticated mechanisms such as biometric verification, hardware tokens, and behavioral analysis. These approaches provide stronger security assurances while maintaining usability for authorized users. Increasingly, organizations are adopting multi-factor authentication (MFA) to strengthen defenses against evolving security threats and to meet stringent regulatory requirements. Following authentication, the authorization phase determines the specific permissions and privileges granted to the verified subject. This process evaluates multiple contextual factors, including the subject's identity, assigned roles, current location, time of access request, and the overall state of the system[47]. Modern authorization systems must strike a careful balance between providing granular access control and maintaining operational efficiency. They are designed to ensure that legitimate users can seamlessly access the resources they need without encountering unnecessary barriers, while still enforcing strong security measures to protect sensitive assets. Achieving this balance

Lead City University Ibadan DO NOT COPY

requires policies and mechanisms that are precise enough to limit access strictly to what is necessary, yet streamlined enough to avoid hindering productivity.

The evolution of access control models mirrors the shifting security requirements and technological landscapes within organizations. Discretionary Access Control (DAC) offers flexibility by allowing resource owners to directly assign and manage access permissions. This approach aligns with natural organizational hierarchies, where information owners retain authority over their resources. However, because permission management is distributed, DAC can introduce administrative complexity and increase the risk of security vulnerabilities if not carefully governed.

In contrast, Mandatory Access Control (MAC) adopts a centralized, policy- driven framework in which system- wide security rules dictate access rights. Under MAC, permissions are determined through formal security labels and clearance levels, ensuring that access decisions are consistent, non- discretionary, and aligned with organizational or regulatory requirements. While MAC enhances control and reduces the risk of unauthorized access, it can be less flexible and more resource- intensive to implement[6]. This model proves particularly effective in environments requiring strict security controls and compliance with specific regulatory requirements. Access control refers to regulating access to the requested resource on a computer or network system[47]. Without access control, there would be no restrictions on who could access resources within an organization, creating significant risks to privacy, security, and compliance. For example, in a healthcare setting, doctors and nurses could view patients' insurance details, insurance companies could access confidential medical records, and research organizations could directly identify study participants, regardless of whether such access was appropriate or lawful. While implementing robust access control measures, organizations ensure that every user is identified, authenticated, and authorized before being

Lead City University Ibadan DO NOT COPY

granted access to resources or permitted to perform operations on a system. This layered process safeguards sensitive information, enforces compliance with legal and ethical standards, and ensures that individuals only have access to the data necessary for their specific role or task[48].

In educational institutions, access control mechanisms are implemented to regulate interactions among key stakeholders, including students, management, parents, academic staff, and non-academic staff. These mechanisms are essential for safeguarding the confidentiality, availability, and integrity of both academic and administrative data and records. In many academic environments, current access control policies operate on the assumption that all potential access requests can be anticipated in advance and managed primarily through authentication. While this approach provides a foundational layer of security, it may not fully address the dynamic and evolving nature of access needs in modern educational systems, particularly in environments where roles, permissions, and data usage patterns change frequently.

Role-Based Access Control (RBAC) has become one of the most widely adopted access control models, aligning permissions with organizational roles and responsibilities. Grouping access rights into roles that correspond to specific job functions or positions, RBAC streamlines permission management while upholding security through the principle of least privilege, ensuring users have only the access necessary to perform their duties. Its proven effectiveness across diverse organizational contexts has led to its broad adoption and ongoing refinement to meet evolving security demands[49]. Recent advancements have introduced more sophisticated approaches, such as Attribute-Based Access Control (ABAC), which evaluates dynamic attributes of subjects, objects, and environmental conditions when making access decisions. This model offers greater flexibility and granularity, enabling organizations to

Lead City University Ibadan DO NOT COPY

implement complex, context-aware policies that adapt to changing operational and security conditions[49]. The rise of Zero Trust architecture has further reshaped access control paradigms by eliminating implicit trust based solely on network location. Instead, it requires continuous verification of every access attempt, regardless of origin, thereby strengthening defenses against insider threats and external breaches.

Emerging trends also include the integration of artificial intelligence (AI) and machine learning (ML) into access control systems. These technologies enhance both security and usability by enabling advanced analysis of access patterns, detecting anomalies in real time, and supporting adaptive policy enforcement based on learned behaviors and risk profiles. Together, these developments represent a shift toward more intelligent, adaptive, and resilient access control frameworks capable of meeting the demands of modern computing environments[49].

The security of databases is far more than a purely technical requirement; it is a cornerstone of institutional integrity, credibility, and trust. Databases often hold the most sensitive and mission-critical information within an organization, ranging from personal records and financial data to intellectual property and strategic plans. Protecting these assets safeguards not only operational continuity but also the institution's reputation, legal compliance, and the confidence of stakeholders[50]. A breach or compromise can have far-reaching consequences, including financial loss, legal liability, reputational damage, and erosion of public trust. Conversely, a robust database security framework, encompassing access control, encryption, auditing, and continuous monitoring, demonstrates an institution's commitment to responsible stewardship of information. In this way, database security is inseparable from the broader principles of accountability, transparency, and ethical governance[50]. Databases, as repositories of highly valuable information, are critical organizational assets that demand

Lead City University Ibadan DO NOT COPY

robust protection mechanisms to defend against a wide spectrum of threats. Among these, insider threats present a particularly serious challenge, as they have the potential to inflict significant damage from within the institution, often with privileged access and intimate knowledge of systems.

The imperative to secure databases arises from the invaluable nature of the data they contain. This information is not only vital for the day-to-day operations of an organization but also represents a substantial portion of its intellectual property and financial capital. A compromise could disrupt operations, erode stakeholder trust, and cause irreparable harm to the institution's reputation and strategic position. For this reason, database security must be approached as a core component of institutional governance, integrating technical safeguards, strict access controls, continuous monitoring, and well-defined policies to ensure the confidentiality, integrity, and availability of critical data assets[50]. Database security encompasses various measures, both technical and procedural, designed to protect databases from unauthorized access, misuse, or theft. These measures include access control mechanisms, encryption, data masking, and implementing security policies and procedures that govern data access and use, thus ensuring data confidentiality, integrity, and availability, principles foundational to information security

Database security is a comprehensive discipline that integrates both technical safeguards and procedural controls to protect databases from unauthorized access, misuse, alteration, or theft. It involves the deployment of mechanisms such as access control systems to regulate who can interact with specific data, encryption to protect information both in transit and at rest, and data masking to obscure sensitive details from unauthorized viewers. Equally important is the establishment of well-defined security policies and procedures that govern how data is accessed, used, stored, and shared within the organization. Together, these measures uphold

Lead City University Ibadan DO NOT COPY

the core principles of information security, confidentiality, integrity, and availability, ensuring that sensitive information remains protected, accurate, and accessible to authorized users when needed[51]. Insider threats refer to security risks originating from individuals within an organization who possess legitimate access to its systems, data, and security protocols. These individuals may include employees, contractors, business partners, or any trusted party with insider knowledge of the organization's operations. Such threats can take multiple forms, ranging from unintentional incidents, such as accidental data leaks caused by negligence, human error, or lack of awareness, to deliberate acts of misconduct, including data theft, system sabotage, fraud, or corporate espionage. The danger posed by insider threats lies in the fact that these actors already have authorized access, making their actions harder to detect and potentially more damaging than external attacks[52].

The impact of insider threats on organizations can be profound, ranging from the compromise of sensitive information to significant financial losses, reputational harm, and even severe legal repercussions[53]. What makes insider threats particularly challenging is that they originate from individuals who already possess legitimate access to the organization's systems, networks, and data. This inherent trust and authorized access allow malicious or negligent actions to bypass many of the defenses designed to stop external attacks. Detecting and mitigating such threats is further complicated by the need to balance robust security measures with the preservation of an open, collaborative, and trusting organizational culture.

Overly restrictive controls can hinder productivity and morale, while insufficient safeguards leave critical assets vulnerable. As a result, effective insider threat management requires a nuanced approach that combines strong technical controls, continuous monitoring, and a culture of security awareness without eroding the trust essential for healthy workplace relationships[53]. Although conventional strategies in combating insider threats emphasize the

Lead City University Ibadan DO NOT COPY

importance of robust access controls, continuous monitoring of user activities, and cultivating a security-aware organizational culture, recent trends and incidents underscore the need for a more nuanced approach. There is an emerging consensus on the importance of behavioral analytics and machine learning techniques in identifying anomalous behavior that may indicate an insider threat, as these technologies complement traditional security measures by providing deeper insights into user behavior, thereby enabling more proactive threat detection and response[53]. Moreover, the role of institutional factors in mitigating insider threats has gained recognition, with factors such as employee satisfaction, transparent communication, and ethical leadership being identified as critical in reducing the likelihood of insider threats[53].

Access control mechanisms have undergone a profound transformation, moving far beyond the simple, static models once sufficient for basic security requirements. Early approaches were primarily designed to manage straightforward access scenarios, often within small, well- defined environments. However, as organizations have grown in scale and complexity, and as cybersecurity threats have become more sophisticated, these traditional models have proven inadequate. Modern access control frameworks are now built to accommodate intricate organizational hierarchies, dynamic workflows, and the diverse range of devices, users, and applications that interact within today's interconnected systems. They are also designed to address nuanced challenges such as insider threats, which require more than just perimeter defenses[54]. The foundational models of access control mechanisms are the Discretionary Access Control (DAC) and Mandatory Access Control (MAC)[55]. DAC, characterized by its flexibility, allows the resource owner to determine who has access to it (like a homeowner who decides which guests can enter their home). However, its reliance on individual users to set their access controls introduces significant risk, particularly with insider threats, as it enables users with malicious intent to grant access to sensitive information improperly[55].

Lead City University Ibadan DO NOT COPY

Mandatory Access Control (MAC) adopts a far more stringent approach than Discretionary Access Control (DAC), relying on a centralized policy framework to determine access rights based on formal classifications and security clearances. This model is comparable to the protocols in a military facility, where access to classified information is strictly regulated according to rank and the necessity of knowledge. While MAC offers a higher degree of protection, particularly against insider threats, its rigid structure can limit operational flexibility and slow down processes within an organization. To address the shortcomings of both DAC and MAC, Role-Based Access Control (RBAC) emerged as a transformative model in access control philosophy. RBAC shifts the focus from individual users or rigid data classifications to the roles defined within an organization, aligning access rights directly with job functions and responsibilities[55].

Role-Based Access Control (RBAC) is grounded in several core principles that collectively enhance security while maintaining operational efficiency. One of these is the principle of Minimum Necessary Access, which ensures that users are granted only the permissions required to carry out their specific roles, thereby reducing the likelihood of unauthorized access to sensitive information. Closely related is the principle of Separation of Duties, which prevents any single individual from performing tasks that could create a conflict of interest or enable fraudulent activity, ensuring that critical processes require oversight or collaboration. RBAC also enforces the Least Privilege principle, restricting access rights to the absolute minimum necessary for a user to perform their job functions[56]. RBAC's role-centric model offers a scalable solution that can adapt to organizational changes, making it a robust framework against insider threats[56]. RBAC comprises several fundamental components, including roles, permissions, sessions, and user-role assignments.

Lead City University Ibadan DO NOT COPY

In Role-Based Access Control (RBAC), roles are established based on the specific job functions within an organization, serving as an abstraction that groups together the actions, responsibilities, and authority associated with those functions. Rather than assigning permissions directly to individual users, RBAC assigns them to roles, which are then mapped to users according to their duties. Permissions represent the access rights or privileges granted to a role, enabling it to perform defined operations on system resources. Sessions act as the operational link between users and their assigned roles, representing the period during which a user is actively operating within the system under one or more roles. This session-based approach allows for flexibility, as users can activate only the roles necessary for a given task, thereby supporting the principle of least privilege and reducing the risk of unauthorized access[56]. In Role-Based Access Control (RBAC), user-role assignments form the critical link between individuals and the permissions they can exercise within a system. This process involves mapping each user to one or more predefined roles that reflect their job functions, responsibilities, or organizational position. These assignments determine the scope of access available to a user and, importantly, which roles they are permitted to activate during a given session[56].

In addition, the architecture of Role-Based Access Control (RBAC) supports a modular and highly adaptable approach to managing access rights. This design allows changes to roles, permissions, or user assignments control to be made independently, without necessitating a complete overhaul of the entire access control framework. Such flexibility is essential for organizations that must frequently adapt to evolving operational needs, whether due to shifts in job functions, restructuring, or personnel turnover[57]. One of the most notable strengths of Role-Based Access Control (RBAC) lies in its capacity to enforce the principles of least privilege and separation of duties, both of which are fundamental to reducing the risk of insider threats. While ensuring that users are granted only the minimum access necessary to

Lead City University Ibadan DO NOT COPY

perform their responsibilities, RBAC minimizes the potential for unauthorized activities, whether intentional or accidental. Its role-centric design also delivers scalability and adaptability, making it well-suited for organizations with large user bases and complex operational structures. When roles are defined according to organizational functions rather than tailored to individual users, permissions management becomes far more efficient. This approach allows administrators to update or modify role permissions centrally, without the need to adjust each user's access rights individually, thereby streamlining administration while maintaining strong, consistent security controls across the organization.

Although Role-Based Access Control (RBAC) is widely regarded as one of the most effective models for managing access rights, its successful implementation can be a demanding process. The core challenge lies in accurately defining roles and mapping them to the appropriate permissions, a task that becomes increasingly complex in organizations with layered hierarchies, overlapping responsibilities, and dynamic operational needs. In such environments, determining the precise boundaries of each role requires a deep understanding of business processes, security requirements, and compliance obligations[58]. This process is often time-consuming, involving extensive analysis, stakeholder consultation, and iterative refinement to ensure that roles are neither too broad, risking excessive access, nor too narrow, causing operational inefficiencies. Furthermore, as organizations evolve, roles and permissions must be continuously reviewed and updated to reflect changes in structure, technology, and regulatory landscapes, making RBAC not just a one-time setup but an ongoing governance commitment.

The dynamic nature of modern work environments, defined by constant shifts in job functions, responsibilities, and organizational priorities, demands that Role-Based Access Control (RBAC) systems remain agile and responsive[59]. As personnel transition between

Lead City University Ibadan DO NOT COPY

roles and operational requirements evolve, it becomes essential to regularly update and refine role definitions and user assignments control to ensure that access rights remain accurate, relevant, and aligned with security policies. In response to these challenges, recent developments in RBAC research and implementation have increasingly emphasized adaptability and intelligence. Innovations such as dynamic role assignment, context-aware access decisions, and integration with real-time analytics are enabling RBAC systems to adjust permissions automatically in line with changing conditions. The incorporation of artificial intelligence and machine learning further enhances this capability, allowing systems to detect anomalies, anticipate access needs, and continuously optimize policies. These advancements are transforming RBAC from a static, rule-driven framework into a proactive, intelligent access control model capable of meeting the complex and rapidly evolving demands of contemporary organizations[59]. Trends such as Dynamic Role-Based Access Control (RBAC) systems, which adjust roles and permissions in real time based on contextual factors like time of day, geographic location, or device type, represent a significant evolution in access control strategies[59]. In parallel, the integration of machine learning algorithms into RBAC frameworks is enabling automatic role assignments, continuous policy optimization, and advanced anomaly detection. These intelligent capabilities allow systems to identify unusual access patterns, predict emerging access needs, and adapt permissions accordingly, often without manual intervention. Together, these advancements directly address some of the traditional limitations of static RBAC models, making them more agile, scalable, and capable of responding to both rapidly changing organizational requirements and increasingly sophisticated threat landscapes.[59].

Role-Based Access Control (RBAC) is considered a strategic framework pivotal in mitigating insider threats, a pressing concern for organizations worldwide[59]. It employs several strategic

Lead City University Ibadan DO NOT COPY

mechanisms that effectively reduce the risk of insider threats[59]. At the core of these strategies lies the principle of least privilege, which dictates that individuals should be granted only the minimum permissions required to perform their specific roles within the organization. Complementing this is the principle of separation of duties (SoD), a critical safeguard within RBAC that ensures no single individual can carry out conflicting tasks that might enable unauthorized or harmful actions. While requiring multiple individuals to complete sensitive processes, SoD not only mitigates the risk of fraud but also reduces the likelihood of errors, adding an essential layer of oversight and accountability[60]. Furthermore, modern RBAC implementations increasingly incorporate dynamic access controls, which adjust permissions in real time based on contextual factors such as the time of access, the user's location, or the nature of the transaction. This adaptability allows organizations to enforce more precise, situationally aware security policies that respond to changing conditions without compromising operational efficiency[60].

The adaptability of Role-Based Access Control (RBAC) is essential in addressing the shifting landscape of insider threats, particularly under high-risk conditions where access rights must be tightened without compromising legitimate operations. While dynamically adjusting permissions in response to contextual cues, RBAC helps ensure that users retain only the access necessary for their roles, thereby minimizing the potential for misuse. Despite its recognized effectiveness in mitigating insider threats, RBAC is not without its limitations. Scholars and practitioners alike have noted that the process of accurately defining and managing roles can be complex and resource-intensive, especially in large organizations with fluid structures and overlapping responsibilities[60]. This complexity can become a barrier to implementation and maintenance, requiring ongoing administrative effort and strategic oversight. Moreover, there is a persistent concern that RBAC, if applied too rigidly, may hinder operational efficiency by restricting access in ways that delay workflows or inhibit

Lead City University Ibadan DO NOT COPY

collaboration. These challenges underscore the importance of treating RBAC as a dynamic framework, one that must be continuously updated, refined, and intelligently adapted to reflect evolving organizational needs and threat conditions. Only through such proactive governance can RBAC remain both secure and functional in today's fast-paced environments[60]. The integration of advanced technologies, such as machine learning and artificial intelligence, is seen as a promising direction for making RBAC more adaptive and effective against sophisticated insider threats.

The implementation of Role-Based Access Control (RBAC) within large-scale institutions, such as a prominent European bank, offers a compelling illustration of its effectiveness in managing access to sensitive information across vast and complex organizational ecosystems[61]. In such environments, where thousands of employees interact with critical systems and customer data daily, RBAC provides a structured and scalable framework for assigning permissions based on clearly defined roles. This role-centric approach ensures that individuals are granted access only to the resources necessary for their specific functions, thereby minimizing the risk of unauthorized data exposure and reinforcing compliance with regulatory standards. Moreover, by centralizing access management around organizational roles rather than individual users, RBAC simplifies administrative overhead and enhances consistency in policy enforcement. The bank's ability to maintain operational efficiency while safeguarding customer trust and institutional integrity underscores the practical value of RBAC as a cornerstone of modern access control strategy[61]. This case study highlights the complexity and strategic depth involved in implementing Role-Based Access Control (RBAC) within a large-scale organization. The establishment of approximately 1,300 distinct roles to serve the operational needs of over 50,000 employees across 1,400 branches exemplifies the meticulous process of role engineering required to align access controls with diverse job

Lead City University Ibadan DO NOT COPY

functions and responsibilities. Such an undertaking demands a structured and methodical framework, capable of capturing the nuances of organizational hierarchies, workflows, and compliance requirements[62]. This example underscores the critical importance of thoughtful role design and ongoing refinement in ensuring that RBAC systems remain scalable, efficient, and responsive to the evolving demands of complex institutional environments[62].

In parallel with other critical sectors, the education industry faced an alarming surge in ransomware attacks during the COVID-19 pandemic, exposing deep vulnerabilities in its digital infrastructure[62]. As institutions rapidly transitioned to remote learning platforms, the attack surface expanded, making schools, colleges, and universities prime targets for cybercriminals. This crisis underscored the urgent need for robust cybersecurity frameworks, particularly those grounded in the principles of zero-trust architecture. Within this model, Role-Based Access Control (RBAC) plays a pivotal role by ensuring that users, whether students, faculty, or administrative staff, are granted only the minimum access necessary for their roles. In higher education environments, where diverse user groups interact across distributed networks, RBAC provides a scalable and auditable structure for managing access rights. Its integration into zero-trust strategies not only strengthens defenses against ransomware but also supports compliance with regulatory standards such as FERPA and HIPAA, making it an indispensable tool in the evolving cybersecurity landscape of academia[62]. The adoption of rigorous security assessments, enhanced system visibility, and comprehensive staff training emerges as critical strategies. Furthermore, the emphasis on data backups as a cornerstone of business continuity and disaster recovery plans highlights the proactive measures required to mitigate ransomware threats, ensuring the protection of sensitive data.

Lead City University Ibadan DO NOT COPY

While Role-Based Access Control (RBAC) is widely recognized for its strategic effectiveness in reducing insider threats through structured and principle-driven access management, its practical implementation and day-to-day operationalization are not without significant challenges[63]. One of the foremost difficulties lies in the initial design and definition of roles, which requires a deep and accurate understanding of organizational workflows, responsibilities, and security requirements. In large or dynamic organizations, this process can become highly complex, as overlapping duties, evolving job functions, and frequent personnel changes demand continual adjustments to role structures and permissions. Additionally, maintaining RBAC over time can be resource-intensive, requiring ongoing governance to prevent role proliferation, privilege creep, and misalignment between access rights and actual job needs.

There is also the risk that, if implemented too rigidly, RBAC may hinder operational efficiency by restricting legitimate access in ways that slow down critical processes. These limitations highlight the importance of coupling RBAC with adaptive strategies, such as periodic role reviews, automation, and integration with contextual or risk-based access controls, to ensure that it remains both secure and operationally effective in the face of evolving organizational and threat landscapes[63]. These obstacles affect the efficiency and effectiveness of RBAC systems and highlight the nuanced complexity of mitigating insider threats within diverse organizational landscapes. For instance, a significantly pressing challenge in implementing RBAC is the phenomenon of role explosion, where the granularity of roles becomes so detailed that managing them becomes impractical[63]. This often occurs in organizations with complex operational structures, requiring a delicate balance between granularity and manageability, resulting in administrative burden, operational inefficiencies and potential security oversights. Furthermore, defining and managing roles can be difficult,

Lead City University Ibadan DO NOT COPY

particularly in dynamic environments where job functions and workflows evolve rapidly. The initial phase of accurately mapping organizational roles to specific permissions is critical. Thus, misalignment can restrict necessary access, hinder job performance, or inadvertently grant excessive privileges, elevating the risk of insider threats. The ongoing management of these roles, including updates and modifications in response to organizational changes, requires dedicated resources and continuous oversight.

While Role-Based Access Control (RBAC) is effective in structuring permissions around clearly defined organizational roles, it has limitations in addressing the complex and evolving nature of insider threats[64]. A key drawback is its static design, where permissions remain fixed once assigned to a role, without accounting for temporal or contextual factors such as time of access, location, device type, or operational risk level. This rigidity can leave gaps in security, as it does not adjust dynamically to unusual patterns or heightened threat conditions. To overcome this, RBAC often needs to be complemented with adaptive, context-aware controls that can modify access in real time based on changing circumstances. For instance, an employee's access requirements may shift depending on variables such as the time of day, their physical location, or their involvement in a specific project, factors that traditional, static RBAC configurations are not designed to address. This lack of contextual adaptability can result in either excessive access during low-risk periods or insufficient access when legitimate needs arise. Another notable limitation is the potential for abuse within the boundaries of defined roles[64].

Role-Based Access Control RBAC inherently assumes that roles are assigned through a trustworthy and well-governed process, with accurate mapping of responsibilities to permissions. However, if role definitions are flawed, overly broad, or influenced by poor oversight, they can inadvertently grant users more privileges than necessary, creating

Lead City University Ibadan DO NOT COPY

opportunities for intentional misuse or accidental security breaches[64]. For instance, an employee's access requirements may shift depending on variables such as the time of day, their physical location, or their involvement in a specific project, factors that traditional, static RBAC configurations are not designed to address. This lack of contextual adaptability can result in either excessive access during low-risk periods or insufficient access when legitimate needs arise. Another notable limitation is the potential for abuse within the boundaries of defined roles. RBAC inherently assumes that roles are assigned through a trustworthy and well-governed process, with accurate mapping of responsibilities to permissions. However, if role definitions are flawed, overly broad, or influenced by poor oversight, they can inadvertently grant users more privileges than necessary, creating opportunities for intentional misuse or accidental security breaches.

However, recent advancements aimed at strengthening Role-Based Access Control (RBAC) against insider threats focus on integrating dynamic access control mechanisms that adjust permissions in real time based on contextual factors such as location, time, or device type. Complementing this, the use of behavioral analytics enables continuous monitoring for unusual activities that may signal malicious intent or policy violations. These innovations make RBAC more adaptable and responsive to evolving access needs and shifting threat landscapes. Furthermore, there is growing recognition that insider threat mitigation is most effective when approached holistically, combining RBAC's structured role management with advanced monitoring tools, employee behavior analysis, and a strong organizational culture of security awareness[65]. This integrated strategy not only enhances technical defenses but also addresses the human and procedural dimensions of security. Such a comprehensive strategy underscores the recognition that while RBAC provides a robust framework for access control, it should be part of a broader security posture that addresses the complexities of insider threats.

Lead City University Ibadan DO NOT COPY

The imposition of stringent regulatory frameworks such as the General Data Protection Regulation (GDPR) has a significant impact on the design and operation of Role-Based Access Control (RBAC) systems, particularly in the context of mitigating insider threats[66]. GDPR's emphasis on data minimization, purpose limitation, and accountability requires organizations to ensure that access rights are strictly aligned with legitimate business needs and that personal data, whether belonging to customers or employees, is only accessible to authorized individuals. This regulatory pressure reinforces the principle of least privilege within RBAC, compelling organizations to define roles with greater precision and to maintain detailed audit trails for compliance verification. At the same time, GDPR introduces operational challenges, as insider threat monitoring must be balanced against privacy obligations, ensuring that surveillance and behavioral analytics do not infringe on the rights of data subjects.

Consequently, RBAC strategies under GDPR must integrate robust governance processes, regular role reviews, and transparent policies that both satisfy regulatory requirements and strengthen defenses against malicious or negligent insider activity[66]. These regulations mandate rigorous controls over who can access sensitive personal and health-related information, necessitating that organizations implement and continuously update their RBAC systems to ensure compliance. GDPR, for example, emphasizes the principle of "data minimization," where access to personal data must be limited to what is strictly necessary for the completion of duties, thereby requiring precise definition and management of roles within RBAC systems[66]. Compliance with these frameworks not only requires a technical alignment of RBAC systems but also an organizational culture that prioritizes data privacy and security. Regular audits, role reviews, and user training become indispensable components of compliance strategies, ensuring that insider threats are identified and mitigated effectively,

Lead City University Ibadan DO NOT COPY

and that data access governance aligns with the legal requirements. Thus, regulatory frameworks like GDPR play a pivotal role in shaping the implementation and effectiveness of RBAC systems in safeguarding sensitive information against insider threats.

Role-Based Access Control (RBAC) has undergone notable technological advancements aimed at strengthening its ability to counter insider threats[67]. Modern implementations increasingly integrate dynamic access control mechanisms that adjust permissions in real time based on contextual factors such as user location, time of access, and device security posture. The incorporation of machine learning algorithms further enhances RBAC by enabling automated role assignments, detecting anomalous behavior, and refining access policies through continuous analysis of user activity patterns. These enhancements address the limitations of traditional static RBAC models, making them more adaptive to evolving operational needs and sophisticated threat vectors. These advancements, driven by the rapid development of computational techniques and algorithms, aim to address some inherent limitations of traditional RBAC systems.

The emergence of Dynamic Role-Based Access Control (DRBAC) marks a significant evolution of the traditional RBAC model by introducing flexibility in role assignments and permissions that adapt to contextual factors such as time, location, or transaction attributes. This real-time adaptability enables organizations to align access rights more closely with operational conditions, thereby reducing the risk of insider threats through situationally aware adjustments. Complementing this, machine learning algorithms are increasingly applied to role mining, analyzing patterns in user activity to automate the definition and assignment of roles based on actual usage. This not only streamlines the role design process but also ensures that assigned roles accurately reflect operational realities, minimizing mismatches between permissions and legitimate needs. Additionally, behavioral analytics has emerged as a

Lead City University Ibadan DO NOT COPY

powerful enhancement to RBAC, monitoring user behavior to detect anomalies that may signal insider threats. When integrated with RBAC, these tools add a proactive layer of defense by identifying and responding to unusual access patterns or transactions, even when carried out by authorized users, thereby strengthening the overall security posture.

The ethical and privacy implications of incorporating behavioral analytics into Role-Based Access Control (RBAC) systems present a complex area that warrants deeper examination[68]. While behavioral analytics can greatly strengthen insider threat detection by identifying unusual patterns of activity, it also introduces legitimate concerns about privacy and the potential for misuse. This underscores the need for research into frameworks that balance robust security measures with ethical safeguards and privacy protections. Role-Based Access Control (RBAC) remains a powerful tool for enhancing database security and mitigating insider threats, yet it is not without its challenges. Effective implementation requires a clear understanding of its limitations, particularly in complex or dynamic environments. Addressing these hurdles calls for a multifaceted approach that blends technical innovations with sound organizational practices. Advancements such as dynamic RBAC, which adapts permissions in real time to reflect operational changes, and the integration of RBAC with behavioral analytics and complementary security controls, can deliver more comprehensive protection. Sustaining this effectiveness depends on ongoing governance, regular audits of roles and permissions, continuous refinement of access policies, and active stakeholder engagement in role definition, to ensure that RBAC remains aligned with both security objectives and operational needs.

Lead City University Ibadan DO NOT COPY

2.2 Theoretical Framework

2.2.1 TRIAD (CIA) Framework

The Triad CIA serves as a foundational framework in information security, defining three core principles that guide the protection of information assets: confidentiality, integrity, and availability[69]. Confidentiality ensures that sensitive information is accessible only to authorized individuals, safeguarding it from unauthorized disclosure. Integrity focuses on maintaining the accuracy, consistency, and trustworthiness of data throughout its lifecycle, preventing unauthorized alterations that could compromise its reliability. Availability ensures that information and critical systems remain accessible to authorized users whenever needed, supporting uninterrupted operations. Together, these principles provide a balanced approach to securing information, forming the basis for designing, implementing, and evaluating effective security policies and controls[69]. This theoretical framework provides organizations with a structured approach to developing comprehensive security programs and evaluating security measures.

Confidentiality represents the first pillar of information security, emphasizing the prevention of unauthorized access to or disclosure of sensitive information. Its core objective is to ensure that data remains private and is accessible only to individuals who have been explicitly granted permission to view or use it. Achieving confidentiality begins with effective data classification, which involves identifying information that requires protection and assigning appropriate security levels. To enforce this principle, organizations employ a range of measures, including encryption for both data at rest and in transit, robust access control systems, secure authentication protocols, and physical safeguards for critical infrastructure. In academic institutions, for example, the confidentiality of student and staff records is a regulatory requirement, necessitating the use of strict access controls, encryption technologies,

Lead City University Ibadan DO NOT COPY

and comprehensive audit trails to protect sensitive academic information from unauthorized exposure.

The technical implementation of confidentiality extends well beyond basic access restrictions, incorporating advanced measures to safeguard sensitive information. Modern systems utilize robust encryption algorithms, secure key management practices, and multi-factor authentication to ensure that even if unauthorized individuals gain system access, the protected data remains unreadable and unusable. Beyond technical safeguards, confidentiality must also be embedded in operational procedures, including the secure handling of printed materials, proper disposal of sensitive documents, and comprehensive employee training to prevent accidental disclosures. The shift toward cloud computing and widespread remote work has further complicated confidentiality management, necessitating additional controls such as Virtual Private Networks (VPNs), endpoint protection solutions, and data loss prevention (DLP) systems. Together, these measures create a layered defense that addresses both technological and human factors in protecting information assets[69].

Integrity, the second pillar of the CIA Triad, ensures that information remains accurate, complete, and unaltered throughout its lifecycle. It safeguards data not only from deliberate tampering but also from accidental changes, thereby preserving consistency and reliability. To uphold this principle, organizations deploy technical controls such as checksums, digital signatures, and version control systems, which detect and prevent unauthorized modifications while maintaining audit trails of legitimate changes. In sectors like finance, integrity controls are critical for ensuring the accuracy of transaction records, often supported by multiple verification steps and reconciliation processes. Effective implementation addresses both data at rest and data in transit, using mechanisms like hash functions and digital signatures to confirm that files remain unmodified during storage or transmission. Database management

Lead City University Ibadan DO NOT COPY

systems further reinforce integrity through transaction controls and rollback capabilities, ensuring consistency during complex operations. Complementary change management processes require that all modifications follow proper authorization and documentation protocols. Integrity also encompasses non-repudiation, which guarantees that the origin of data can be verified and that actions cannot be denied after they have been performed[69].

Availability, the third pillar of the CIA Triad, focuses on ensuring that information and systems remain accessible to authorized users whenever needed. Achieving this requires organizations to build resilient infrastructures supported by redundancy measures and disaster recovery capabilities. High-availability environments often incorporate redundant hardware, backup power supplies, and multiple network connections to eliminate single points of failure. Performance considerations are equally important, as systems must be capable of handling expected workloads while maintaining acceptable response times. The adoption of cloud services and distributed architectures has introduced new dimensions to availability, making the careful management of service level agreements, backup strategies, and failover mechanisms essential. In practice, availability is reinforced through comprehensive business continuity planning and disaster recovery procedures, which include regular backups, alternate processing sites, and periodic testing of recovery plans. The growing prevalence of ransomware attacks has further underscored the need for robust backup systems and network isolation measures to safeguard critical data and maintain uninterrupted operations, even in the face of severe disruptions[69].

The interplay between confidentiality, integrity, and availability demands a deliberate and well- considered balance, as enhancing one principle can inadvertently affect the others. For instance, implementing stronger encryption to reinforce confidentiality may introduce processing overhead that impacts system performance and, consequently, availability.

Lead City University Ibadan DO NOT COPY

Likewise, enforcing stringent integrity controls can limit accessibility for legitimate users, potentially hindering operational efficiency. For Oyo State-owned Polytechnics, achieving this balance requires a thorough assessment of institutional security needs, operational priorities, and acceptable risk levels. While clearly defining these parameters, decision-makers can determine the most appropriate trade-offs, ensuring that security measures are both effective in protecting information assets and practical in supporting the institution's academic and administrative functions.

The interplay between confidentiality, integrity, and availability demands a deliberate and well-considered balance, as enhancing one principle can inadvertently affect the others. For instance, implementing stronger encryption to reinforce confidentiality may introduce processing overhead that impacts system performance and, consequently, availability. Likewise, enforcing stringent integrity controls can limit accessibility for legitimate users, potentially hindering operational efficiency. For Oyo State-owned Polytechnics, achieving this balance requires a thorough assessment of institutional security needs, operational priorities, and acceptable risk levels.

Confidentiality is a critical responsibility for Non-Academic Staff, as they handle highly sensitive information that must be safeguarded from unauthorized access. Student records, containing personal details, academic performance, and financial data, are attractive targets for both cybercriminals and potential insider threats. Under the CIA framework, confidentiality is reinforced through measures such as access control lists, strong password policies, multi-factor authentication (MFA), and robust encryption for data at rest and in transit. The application of Role-Based Access Control (RBAC) further strengthens this principle by ensuring that staff can only access information directly relevant to their duties, thereby reducing the risk of data breaches. Compliance with regulations such as the General

Lead City University Ibadan DO NOT COPY

Data Protection Regulation (GDPR) and local data protection laws also demands strict adherence to privacy standards, helping to protect both the institution's reputation and the rights of students and faculty.

Integrity, the second pillar of the CIA framework, ensures that the data managed by Non-Academic Staff remains accurate, consistent, and free from unauthorized alterations. In tertiary institutions, the integrity of academic records is paramount; altered grades or falsified transcripts can damage institutional credibility and lead to serious legal consequences. To uphold integrity, organizations employ tools such as hashing, digital signatures, and version control systems to detect and prevent unauthorized changes. Regular audits and intrusion detection systems help identify suspicious activity, while cybersecurity awareness training equips staff to recognize and resist phishing or social engineering attempts that could compromise data.

Availability, the third pillar of the CIA framework, ensures that data and systems remain accessible to authorized users whenever needed, which is vital for the operational efficiency of Non-Academic Staff. Disruptions caused by cyberattacks, such as Distributed Denial of Service (DDoS) incidents, hardware failures, or ransomware can halt essential functions like student registration, transcript issuance, and financial aid processing. To safeguard against such interruptions, the CIA framework emphasizes measures including system redundancy, regular backups, and comprehensive disaster recovery planning. Cloud-based backups and redundant servers help maintain operations during outages, while staff training on identifying and responding to threats, such as early signs of ransomware, strengthens resilience.

The CIA Triad's relevance is further strengthened by its close alignment with risk management practices, providing a structured approach for identifying, assessing, and mitigating threats. For Non-Academic Staff in Oyo State-owned polytechnics, the threat

Lead City University Ibadan DO NOT COPY

landscape is increasingly complex, encompassing phishing attacks, malware, and insider threats, all intensified by the growing digitization of academic and administrative records. While applying the CIA framework, institutions can conduct targeted risk assessments to pinpoint vulnerabilities, evaluate their potential impact, and implement controls tailored to operational realities. For instance, identifying outdated software as a weakness could prompt timely upgrades, thereby improving both availability and integrity. Moreover, the framework's straightforward structure makes it accessible to non-technical staff, enabling them to actively participate in cybersecurity efforts through regular training, adherence to established policies, and vigilance in daily operations. This combination of technical and human-centric measures ensures a more resilient security posture across the institution.

2.2.2 Records Continuum Model

In an article titled "A Chinese view of Records Continuum Methodology and Implications for Managing Electronic Records," a scholar noted the evolution of the concepts of records continuum had three periods as origins of the continuum concept, wide use of the word 'continuum'; and the formulation and implementation of records continuum model to electronic and paper records management[70]. The declaration that records managers or Non-Academic Staff are the "true archivists" reflects a perspective that emphasizes the continuum of recordkeeping from creation to preservation[71]. It positions archival science not merely as the custodianship of historical materials, but as a discipline fundamentally concerned with the entire lifecycle of records, from their active use in organizational processes to their long-term preservation. In this view, archival science should focus on studying the characteristics of recorded information, the systems that govern record creation and maintenance, and the classification processes that ensure records remain organized, retrievable, and meaningful over time. This approach aligns closely with the records continuum model, which sees no

Lead City University Ibadan DO NOT COPY

rigid divide between records management and archival work, but rather a seamless process where Non-Academic Staff play a pivotal role in safeguarding the authenticity, reliability, and accessibility of information from the moment it is created[71]. This view promoted the search for continuity between archives and data handling.

In the second period, the term continuum was not yet in common use within Australian recordkeeping circles during the mid- 1980s, until Canadian archivist Jay Atherton explicitly introduced it at the 1985 annual conference of the Association of Canadian Archivists. Atherton emphasized that all stages of recorded data are interconnected, forming a seamless continuum in which both Non-Academic Staff and archivists participate, albeit to varying degrees, in the ongoing management of records. He challenged the traditional notion of a linear records life cycle, arguing instead that the stages it described were not discrete, one-time events but rather a series of recurring and interdependent activities. These activities reverberate across both archival practice and records management policy, underscoring the need for continuous collaboration and integrated approaches to the stewardship of information throughout its existence. The underlying unifying factor in the records continuum is its fundamental function of serving both the creators of data and all subsequent users[71]. This perspective positions recordkeeping not as a static, end- stage archival activity, but as an ongoing service that supports the needs of those who generate records while ensuring their continued accessibility, reliability, and relevance for future stakeholders. This perspective highlighted a key weakness in the traditional lifecycle model, the artificial separation between data handling during a record's active phase and archives administration once it was deemed inactive. Such a division often led to fragmented responsibilities, inefficiencies, and gaps in preserving the evidential and informational value of records. In response, the third period of development in the 1990s saw the formulation of the records continuum as a

Lead City University Ibadan DO NOT COPY

conceptual model, most notably articulated by Frank Upward and colleagues at Monash University[72].

The Records Continuum Model is built on four key principles that together present a holistic approach to recordkeeping. First, it adopts an inclusive concept of a "record," encompassing those of continuing value, archives, and recognizing their use for transactional, evidentiary, and memory purposes. This principle unifies approaches to archiving and recordkeeping, whether records are preserved for only a moment or for centuries. Second, it emphasizes viewing records as logical rather than physical entities, focusing on their informational value and context regardless of whether they exist in paper or electronic form. Third, it underscores the institutionalization of the recordkeeping profession's role, highlighting the need to integrate recordkeeping into both business processes and broader societal functions to ensure it is embedded from the outset rather than treated as an afterthought. Finally, it positions archival science as the foundation for organizing knowledge about recordkeeping, acknowledging that such knowledge is dynamic and revisable, yet capable of being structured and applied to guide actions in the past, present, and future. Together, these principles create a framework that supports continuous, integrated, and purpose-driven management of records across their entire existence.

The Records Continuum Model comprises four stages, creation, classification, scheduling, and maintenance and use of information, contrasting with the eight stages of the traditional life-cycle theory. Unlike the life-cycle approach, it positions archivists and Non-Academic Staff as active participants in all stages of record management. This integrated involvement ensures the creation of accurate records containing the right information in the correct formats, the organization of records to facilitate efficient use, the systematic disposal of records no longer needed, and the protection and preservation of those with continuing value.

Lead City University Ibadan DO NOT COPY

As a variation of the life-cycle concept, the continuum model adopts a higher-order intellectual perspective, emphasizing an interconnected process rather than discrete, sequential stages. It underscores the importance of involving records professionals from the earliest planning phases of information systems, particularly in the management of electronic records. While acknowledging that records pass through identifiable stages, the model treats these stages as reference points rather than rigid functions, allowing flexibility in application. This approach enables Non-Academic Staff and archivists to operate at the stages most relevant to their roles, achieving different yet complementary objectives in the stewardship of records.

Given that this study focuses on data handling stages, the Records Continuum Model is considered the most suitable framework. It offers a seamless and dynamic approach to managing data that transcends time and space, ensuring that information is captured and maintained for as long as it is needed to meet academic, administrative, regulatory, social, and cultural requirements. Over time, the model has gained global recognition as a best practice for managing both paper and electronic records. Its advantages over the traditional life-cycle model lie in its integrated mechanism, which unifies the management of documents, data, and archives into a single, cohesive process. While promoting integrated approaches, integrated control, and an integrated framework, it supports the creation of best practice standards. This holistic applicability makes the Records Continuum Model particularly relevant for studies addressing the management of diverse record formats, providing a robust theoretical foundation for effective and sustainable data and archives management.

However, in adopting this theory, the researcher acknowledged the doubts and criticisms that have been raised against it. The Records Continuum Model has, in certain areas, sparked concern and resistance within the data and archives sector. These reactions stem largely from

Lead City University Ibadan DO NOT COPY

the perception that the model's underlying notions blur the traditional boundaries between the roles of Non-Academic Staff and archivists. While advocating for shared involvement across all stages of recordkeeping, the model challenges the long-standing division of responsibilities, leading some professionals to fear that their distinct territories and competencies could be diminished. This perceived overlap has been interpreted as a potential threat to professional autonomy, prompting apprehension among those accustomed to the clearer role demarcations of the traditional life-cycle approach.

This theory directly supports the need for trustworthy, verifiable data in Oyo State-owned polytechnics, where the accuracy of records is fundamental to maintaining academic integrity and meeting regulatory obligations. Within the Capture dimension of the Records Continuum Model, records are formally registered into institutional systems to serve as authoritative evidence of activities and decisions. For Non-Academic Staff, this process typically involves entering student information into databases or enterprise platforms such as Student Information Systems (SIS). A continuum-based policy strengthens this process by ensuring that records are captured in a way that preserves their contextual linkages, for example, associating a transcript not only with the student's name but also with their enrollment history, academic program, and relevant administrative actions. To achieve this, policies would mandate the use of metadata standards, including timestamps, user IDs, course codes, and other identifiers, so that every record is both traceable and verifiable. Such measures are critical for auditability, enabling the institution to respond effectively to regulatory reviews, accreditation checks, or legal inquiries. While embedding these practices into daily operations, Non-Academic Staff can ensure that records are not only accurate and complete but also defensible as authentic evidence of institutional processes, thereby reinforcing trust in the polytechnic's academic and administrative systems.

Lead City University Ibadan DO NOT COPY

The organized dimension of the Records Continuum Model is centered on structuring records in a way that supports their ongoing accessibility, usability, and security within the institution. For non-academic staff, this involves managing a wide range of datasets, such as admissions, grades, and financial aid records, that must be systematically arranged to meet both operational and compliance requirements. Data handling stages grounded in the continuum model would emphasize systematic classification, secure storage, and granular access controls to ensure that records are both protected and easy to locate when needed. For example, implementing role-based access control (RBAC) ensures that only authorized personnel can view or modify sensitive information, aligning with confidentiality obligations under frameworks like the GDPR or relevant local data protection laws. To safeguard integrity, policies could require version control systems and audit trails, enabling the detection and prevention of unauthorized changes to critical records such as grades or certifications.

The Pluralize dimension of the Records Continuum Model extends the value of records far beyond their immediate operational use, ensuring they remain accessible to a wider range of stakeholders and for long-term purposes such as institutional memory, research, and historical preservation. For Non-Academic Staff, this can involve archiving records for accreditation reviews, alumni verification, or institutional history projects. A continuum-based policy would establish clear archiving protocols, ensuring that records are preserved in formats that remain accessible over time, such as through periodic data migration to prevent technological obsolescence. It also reinforces compliance with legally mandated retention schedules, striking a balance between retaining records for regulatory or evidentiary purposes and securely disposing of outdated data to protect privacy.

Lead City University Ibadan DO NOT COPY

The relevance of the Records Continuum Model in Oyo State-owned polytechnics lies in its capacity to effectively address the multifaceted challenges of modern data management. In today's hybrid environment, Non-Academic Staff handle records that are generated, stored, and accessed across multiple platforms, ranging from cloud-based Student Information Systems (SIS) to traditional physical archives. The model's fluid and integrated approach supports the development of policies that seamlessly bridge these digital and physical domains. For instance, it can guide the implementation of regular cloud backups to safeguard availability during system outages, while also enforcing secure disposal protocols for physical records to prevent unauthorized disclosure. This adaptability is essential for mitigating contemporary risks such as cyberattacks, accidental data loss, and unauthorized access, threats that are increasingly prevalent in institutions entrusted with sensitive student information.

Moreover, the Records Continuum Model fosters a proactive rather than reactive approach to data handling, enabling institutions to anticipate and prepare for the future needs of their records from the moment they are created. While embedding the model's principles into institutional policies, Non-Academic Staff are equipped to consider potential future uses, such as compliance audits, accreditation reviews, or stakeholder information requests, at the point of record creation. This forward-thinking mindset minimizes inefficiencies like duplicate data entry or misplaced records, while strengthening confidence in the institution's overall data governance framework. For example, implementing a policy that mandates consistent metadata tagging at the point of capture ensures that records remain contextually rich, traceable, and usable for years to come. Such measures not only support long-term initiatives like longitudinal research and institutional reporting but also safeguard the institution's ability to demonstrate accountability, accuracy, and compliance over time.

Lead City University Ibadan DO NOT COPY

2.2.3 Role–Based Access Control (RBAC) Model

Access control mechanisms have undergone a profound transformation, moving from simple, static models to highly adaptive frameworks capable of addressing the intricate realities of modern cybersecurity[73]. This model uses role definition, permission allocation control, session management and user assignment control. Early approaches, such as Discretionary Access Control (DAC) and Mandatory Access Control (MAC), were effective for straightforward environments but lacked the flexibility to handle the layered permissions and dynamic contexts of today's organizations[73]. The introduction of Role-Based Access Control (RBAC) marked a major step forward, allowing permissions to be assigned based on job functions rather than individual identities, streamlining administration and reducing errors. However, as organizational structures became more complex and threats more sophisticated, particularly from insiders, RBAC's static nature revealed limitations. This led to the emergence of Dynamic RBAC (DRBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC), which incorporate contextual factors such as time, location, device type, and risk level into access decisions. These models enable real-time, fine-grained authorization, ensuring that access rights adapt to changing conditions and potential threats.

To counter insider risks, modern access control strategies integrate behavioral analytics, machine learning–driven anomaly detection, and continuous authentication. These enhancements allow systems to detect unusual patterns, such as atypical data access volumes or attempts to retrieve sensitive files outside normal working hours, and respond automatically by restricting access or triggering alerts. In essence, access control has evolved from being a static "gatekeeper" to functioning as an intelligent, context-aware security layer

Lead City University Ibadan DO NOT COPY

that not only enforces least privilege but also actively monitors and adapts to emerging risks, making it a cornerstone of contemporary cybersecurity resilience.

Discretionary Access Control (DAC) and Mandatory Access Control (MAC) represent two fundamentally different philosophies in managing access rights, each with distinct strengths and weaknesses. DAC offers flexibility by allowing the resource owner to decide who can access their resources, much like a homeowner choosing which guests to admit. This adaptability can be advantageous in dynamic environments, but it also introduces significant risks, particularly from insider threats. Because individual users control permissions, a malicious or careless insider could improperly grant access to sensitive information, undermining security.

In contrast, MAC enforces a far more rigid structure, with access decisions dictated by a centralized policy based on predefined classifications and security clearances. This is akin to a military facility where entry to classified areas is strictly controlled according to rank and the "need-to-know" principle. MAC's centralized control greatly reduces the likelihood of unauthorized access, especially from insiders, but its inflexibility can slow operations and limit efficiency, particularly in organizations that require rapid, adaptive collaboration. In practice, many modern systems adopt hybrid or context-aware models, such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), to balance DAC's flexibility with MAC's security rigor, aiming to achieve both operational agility and strong protection against evolving threats.

In response to the inherent limitations of Discretionary Access Control (DAC) and Mandatory Access Control (MAC), Role-Based Access Control (RBAC) emerged as a transformative shift in access control philosophy. Rather than basing permissions on individual user discretion, as in DAC, or rigid classification levels, as in MAC, RBAC

Lead City University Ibadan DO NOT COPY

centralizes access management around defined organizational roles. Each role is assigned a specific set of permissions aligned with the responsibilities and functions it represents, and users inherit these permissions by virtue of their role assignment[74]. This alignment between access rights and the organization's structure streamlines security administration, making it easier to onboard, reassign, or remove users without manually adjusting individual permissions. It also reduces the likelihood of privilege creep, where users accumulate unnecessary access over time, and minimizes the risk of insider threats by ensuring that individuals can only access the resources necessary for their duties[74]. RBAC operates on several fundamental principles, including Minimum Necessary Access, which provides that users are granted only the access necessary to perform their roles, limiting the potential for unauthorized access to sensitive information; Separation of Duties, which ensures that no single user can perform conflicting tasks; and Least Privilege which restricts access rights to the bare minimum needed to perform their jobs, reducing the risk surface for insider threats.

Role-Based Access Control's (RBAC) role-centric model offers a scalable solution that can adapt to organizational changes, making it a robust framework against insider threats. RBAC comprises several fundamental components, including roles, permissions, sessions, and user-role assignments[74]. In Role-Based Access Control (RBAC), access is organized around roles that reflect specific job functions. Each role carries a set of permissions that define what actions can be performed, and users are assigned to roles based on their responsibilities. When a user logs in, they operate within a session that temporarily links them to the permissions of their assigned role. This setup makes it easy to adjust access, roles, permissions, and user assignments control can be updated independently without overhauling the whole system. That flexibility is especially useful when job duties change or staff leave, allowing organizations to adapt quickly while keeping security intact. One of the most

Lead City University Ibadan DO NOT COPY

significant advantages of RBAC is its ability to enforce the principle of least privilege and separation of duties, which are foundational elements in mitigating insider threats[74]. RBAC's role-centric design makes it both scalable and flexible, allowing organizations to manage access efficiently even in environments with large user bases and complex structures.

In today's fast-changing work environments, where job duties and responsibilities shift frequently, RBAC requires ongoing review and adjustment to remain effective. Recent research and industry developments are pushing RBAC toward greater adaptability and intelligence, integrating capabilities like context-aware policies, machine learning-driven anomaly detection, and hybrid models that combine RBAC with Attribute-Based Access Control (ABAC). These innovations aim to make RBAC more dynamic, responsive to real-time conditions, and better equipped to handle modern security challenges such as insider threats, cloud-based operations, and the demands of zero-trust architectures.[75]. Dynamic Role-Based Access Control (RBAC) represents one of the most promising evolutions of traditional access control, introducing adaptability by adjusting roles and permissions in real time based on contextual factors such as time of day, geographic location, device type, or even current threat levels. This context-aware approach ensures that access rights are not static but instead reflect the operational environment and security posture at any given moment. A key driver of this shift is the integration of machine learning algorithms, which can automate role assignments by analyzing patterns in user behavior, job functions, and access history. These systems can also perform anomaly detection, flagging or restricting unusual activity, such as attempts to access sensitive data outside normal working hours or from unfamiliar locations, before it escalates into a security incident.

Role-Based Access Control (RBAC) is considered a strategic framework pivotal in mitigating insider threats, a pressing concern for organizations worldwide[75]. RBAC incorporates key

Lead City University Ibadan DO NOT COPY

strategies to limit the risk of insider threats. At its core is the principle of least privilege, which grants users only the access they need to perform their specific duties, nothing more. By restricting unnecessary permissions, the likelihood of intentional misuse or accidental data exposure is greatly reduced. Another vital safeguard is separation of duties (SoD), which ensures that no single individual can carry out conflicting tasks that might enable fraud or unauthorized actions. Instead, sensitive processes require the involvement of multiple people, creating built-in checks and balances. Together, these measures strengthen internal security, reduce opportunities for abuse, and help maintain the integrity of critical systems and data.

Role-Based Access Control (RBAC) also incorporates dynamic access controls that adjust permissions based on contextual factors such as time, location, or transaction context[75]. RBAC's adaptability is vital for countering evolving insider threats, as it allows access rights to be tightened in high-risk situations while still aligning with organizational needs. While widely praised for its ability to limit such threats, RBAC is not without its challenges. Defining and managing roles can be complex and resource-intensive, particularly in large or fast-changing organizations. Critics also caution that, if applied too rigidly, RBAC can slow operations and reduce flexibility. Because insider threats continue to evolve, RBAC frameworks must be regularly reviewed, updated, and fine-tuned to remain effective. Emerging approaches that integrate machine learning and artificial intelligence offer promising solutions, automating role assignments, detecting anomalies in user behavior, and adapting permissions in real time. These enhancements aim to make RBAC more responsive, context-aware, and resilient against increasingly sophisticated internal security risks.

In Oyo State-owned polytechnics, Non-Academic Staff handle a wide range of responsibilities, from processing admissions to managing grades, issuing certifications, and administering financial aid. These duties involve working with sensitive personal and

Lead City University Ibadan DO NOT COPY

academic information, which must be protected to maintain confidentiality and integrity in line with regulations such as the GDPR or relevant local data protection laws. Role-Based Access Control (RBAC) supports this by assigning permissions according to clearly defined roles, such as admissions officer, records clerk, or financial aid administrator. For instance, an admissions officer may be able to view and process application forms and personal details but have no access to academic transcripts, while a records clerk might update grade entries but be restricted from viewing financial records. This granular, role-specific control ensures that each staff member can carry out their responsibilities without unnecessary exposure to unrelated or highly sensitive data.

The relevance of RBAC is further underscored by its ability to mitigate insider threats, a significant concern in Oyo State-owned polytechnics, where staff have legitimate access to systems. Limiting access to only what is necessary for a role, RBAC minimizes the potential for misuse, whether intentional or unintentional. For instance, a temporary staff member assigned a limited role would be restricted from accessing sensitive historical records, preventing unauthorized modifications or disclosures. This principle of least privilege, inherent in RBAC, ensures that even if credentials are compromised, the scope of damage is contained, protecting both the institution and its stakeholders.

Role-Based Access Control (RBAC) also enhances operational efficiency for Non-Academic Staff. In busy registry departments, managing access manually for each individual can be time-consuming and error-prone, especially in large institutions with hundreds of staff and thousands of students. RBAC streamlines this by grouping permissions into predefined roles, allowing administrators to assign or revoke access quickly as staff join, change roles, or leave the institution. For example, when a new registrar is on boarded, they can be assigned the "registrar" role, instantly granting access to relevant systems without needing to configure

Lead City University Ibadan DO NOT COPY

permissions individually. This scalability simplifies user management, reduces administrative overhead, and ensures consistency in access control across the institution.

Compliance with legal and regulatory requirements is another area where RBAC delivers significant value. In Oyo State-owned polytechnics, strict data protection standards demand tight control over who can access personal information and the ability to prove that such access is properly managed. RBAC supports this by clearly mapping permissions to specific roles, creating an auditable trail that shows exactly who had access to what data and when. For example, during a GDPR or local data protection audit, RBAC system logs can demonstrate that only authorized personnel, such as designated Non-Academic Staff, accessed student records, and that their permissions were consistent with their job responsibilities. This level of transparency not only simplifies the audit process but also reinforces accountability, helping to build and maintain trust among students, faculty, and regulatory bodies.

2.3 Review of Empirical Studies

2.3.1 Data Handling Stages and Information Security

Empirical evidence underscores that well-defined data handling stages are critical in reducing the risks of data breaches and unauthorized access. It clearly set out procedures for the collection, processing, storage, and secure disposal of information, ensuring that every stage of the data lifecycle aligns with regulatory requirements[76]. Studies show that institutions with structured data handling protocols tend to experience fewer security incidents, as these frameworks promote consistency, accountability, and compliance. One scholarly study, for example, highlights the importance of classifying data according to sensitivity levels and implementing strict access protocols for each category, particularly in

Lead City University Ibadan DO NOT COPY

polytechnic environments where both personal and academic records are managed[76]. This classification not only aids in protecting sensitive data but also aligns with legal frameworks such as the Data Protection Act.

A study on academic libraries in Pakistan examined how aware library staff were of digital information security management (DISM) and the policies guiding it. Conducted in selected public and private university libraries in Lahore, the research gathered data through structured interviews with 15 academic librarians[77]. The study employed a quantitative approach, using interviews across fifteen academic libraries to assess awareness and engagement with digital information security management. The findings revealed a concerning trend: many information specialists and library staff showed limited interest in digital security issues, which directly contributed to their low participation in training programs related to information protection. This lack of engagement suggests a gap in professional development and institutional prioritization of cybersecurity within library environments.

To underscore the broader implications of this issue, the study incorporated a case analysis of King Abdulaziz University Library in Jeddah. This case highlighted the critical need to address the security and safety of library technologies, staff, and patrons. It emphasized that without proactive policies and training, libraries remain vulnerable to digital threats that could compromise sensitive data and disrupt services. The research ultimately calls for stronger institutional frameworks, increased awareness, and targeted capacity-building to ensure that academic libraries can safeguard their digital assets effectively[78]. The study adopted the interview method, and the study sample consisted of administrative and technical officers at the library. The study revealed that libraries and their information systems face notable security and safety risks, many of which stem from outdated practices and

Lead City University Ibadan DO NOT COPY

insufficient oversight. It emphasized that these vulnerabilities can be addressed by adopting modern technologies and crafting well-defined policies tailored to digital environments. At King Abdulaziz University Library, the findings pointed to a lack of consistent monitoring of library collections, which increases exposure to potential threats. Additionally, the study identified shortcomings in the library's written policies and highlighted the absence of a dedicated team to oversee automated systems, both of which contribute to gaps in digital security management. Interestingly, the research also noted that the newer library building had resolved several physical infrastructure issues present in the older facility, such as ceiling leaks and outdated electrical systems, suggesting that physical upgrades can complement digital improvements in creating a safer, more secure library environment.

In a study that aimed to measure the adequacy of the security measures in the network of Umm Al-Qura University libraries[79]. The study, which used interviews with key personnel, including the library director, IT staff, and network administrators, revealed a mixed approach to information security within the university's library system. While the Deanship of Library Affairs showed commitment to securing the physical infrastructure, such as the location and hardware extensions, several critical gaps were identified in digital protection measures.

Notably, the absence of essential safeguards like firewalls, encryption systems, and backup power solutions left the network vulnerable. The study also highlighted operational weaknesses, including irregular updates to antivirus software, inconsistent backup scheduling, lack of staff training on cybersecurity practices, and poor enforcement of password protection protocols. These shortcomings point to a need for a more comprehensive and proactive security strategy, one that combines physical safeguards with robust digital defenses and ongoing staff education to ensure the integrity and resilience of library information systems.

Lead City University Ibadan DO NOT COPY

A study aimed to recognize the status quo of information security systems in Omani libraries. It focused on the main library at Sultan Qaboos University as a model for Omani libraries[80]. The study conducted at Sultan Qaboos University revealed several critical gaps in the management of automated systems within the main library and the university's information systems center. One of the key findings was the lack of centralized oversight for the security of the library's automated systems, which led to inconsistencies and weaknesses in the protection measures in place. While the information systems center had policies to address certain risks, such as hacking and database loss, there were no provisions for other foreseeable threats like sudden power outages, leaving the systems vulnerable to disruption.

Additionally, the study highlighted concerns about data safety within the library's automated system, Symphony, pointing to inadequate follow-up and oversight. Perhaps most concerning was the absence of a formal, written policy outlining safety and security procedures for these systems. Without such documentation, it becomes difficult to enforce standards, train staff effectively, or respond consistently to emerging threats. These findings underscore the urgent need for comprehensive, centralized policies and contingency planning to safeguard digital assets and ensure the resilience of library operations.

In study on the assessment of university library security management. The study sample consisted of 60 staff members from 4 university libraries in Nigeria[81]. The study revealed that academic libraries in three southwestern Nigerian universities lacked formal information security policies and plans. Physical security measures were also weak, with no alarms to prevent theft. Additionally, staff members showed low awareness of security practices. The research emphasized the importance of vigilant library staff and users in safeguarding public resources. It aimed to assess the state of electronic security systems in these institutions, highlighting the need for improved security infrastructure and awareness[82]. The study

Lead City University Ibadan DO NOT COPY

involved 109 participants, including librarians, technical services heads, and other staff from Covenant University, Babcock University, and the University of Lagos, with 81 responses recorded. Findings showed that academic libraries face security challenges and need to strengthen their security services to protect information systems. All three universities had electronic security systems in place. Respondents from Babcock confirmed that CCTV cameras were functioning well, while those from Covenant and UNILAG reported effective gate-mounted cameras. Despite these systems, the study also noted incidents of office materials being taken illegally.

The study aimed to examine security management practices and strategies for preventing book theft in university libraries, using Benue State University Library as a case study. It focused on identifying the causes of theft and proposing solutions to safeguard library resources and ensure their continued availability for users[83]. The study involved 48 library staff members, with 30 responses collected. Findings showed that books in the university library were vulnerable to theft and damage due to weak security measures, lack of office materials, and financial constraints. Separately, a descriptive study was conducted on library and information science departments in Iraqi universities to assess students' awareness of information security and how it relates to their academic coursework[84]. The study used a questionnaire to gather data and found that computing course curricula lacked fundamental concepts of information security. It also revealed gaps in students' awareness of protection practices. However, despite these shortcomings, students still applied protection measures at an average level.

A study was conducted to assess the current state of information systems security management in technical colleges across the Gaza Strip[85]. It focused on evaluating existing security practices, identifying gaps, and understanding how well these institutions are

Lead City University Ibadan DO NOT COPY

prepared to handle digital threats. The findings aimed to inform improvements in policy, infrastructure, and staff awareness to strengthen overall information security[85]. The study involved 180 staff members working in information systems across technical colleges. Findings showed that the infrastructure for information systems was only moderately developed, and there were no clear security policies in place. Commitment to using these systems varied among institutions. The study also found statistically significant differences in how staff perceived the current state of information systems security.

Another study focused on identifying methods and procedures to protect main networks and their information sources, including transferred data, and verifying potential data loss[86]. The study focused on staff involved in computer network protection, including department heads and personnel from information centers in both public and private educational institutions in Riyadh. The sample included 105 engineers, administrators, and technicians responsible for managing hardware and software security. Findings showed that these institutions use various protective tools, such as proxies, firewalls, central distributors, wireless access points, antivirus systems, and internet usage monitoring to safeguard their networks. The study found that half of the institutions had specific plans for firewalls, servers, and routers, which were updated periodically. However, they lacked an integrated system for managing information security. Weaknesses included outdated firewall systems, underperforming antivirus devices, inexperienced security staff, low user professionalism, and the absence of a formal protection policy. Recommendations included hiring information security specialists, training system security staff, establishing clear IT procedures, and improving staff income.

A scholar conducted a study to assess the self-efficacy of information security systems in Florida libraries[87]. The findings showed that professionals with IT training had stronger confidence and better performance in managing security measures[87]. The study explored how

Lead City University Ibadan DO NOT COPY

the educational readiness of librarians affects the implementation of information security systems in Florida libraries. It involved 56 respondents from academic and public libraries. Findings showed that librarians with prior IT training were more effective in applying security measures. While the proposed model wasn't fully supported, the study confirmed a strong link between previous training and self-efficacy, which influenced implementation success. Gender had a weak correlation, and regression analysis showed no predictability. Work experience was a better predictor than IT training, though not as strong as self-efficacy. The study recommended training staff and improving their expertise in information systems security.

The study conducted by a scholar aimed to assess information security management in Malaysian academic libraries[88]. The study involved 39 staff members responsible for information systems in Malaysian academic libraries. It assessed security using five standards: technological measures, policies, procedures, means of security, and awareness activities. Findings showed that device-related threats (70%), human risks (66%), and environmental threats (51%) were most common. Issues included poor device maintenance, use of unauthorized devices, and virus exposure. Differences in security practices were linked to budget, system availability, and staffing. The study recommended implementing organizational measures, noting that technology alone is not enough to address information security challenges.

In a study conducted in Malaysia, aimed to identify the status quo of information systems security in public and private libraries[89]. The study involved 50 staff members responsible for information systems security in Malaysian private and public libraries. It found that 95% of libraries had achieved a high level of electronic security. However, 54% showed weak organizational measures, including inadequate security procedures, lack of administrative

Lead City University Ibadan DO NOT COPY

tools, and limited awareness activities. This weakness was attributed to an overreliance on technology as the sole solution for security.

Data handling stages and information security are interdependent. Information security relies on both elements to classify, protect, and manage data effectively. A complete strategy includes technical tools like encryption and intrusion detection, along with administrative measures such as staff training and awareness programs. Building a culture of security awareness further enhances institutional protection. Effective information security depends on clear data handling policies that guide proper classification and management of information. A strong security strategy combines technical tools, like encryption and intrusion detection, with administrative measures such as staff training and awareness programs[89]. Data handling stages establish the framework for how data is managed throughout its lifecycle. These policies define the processes for data collection, storage, processing, and disposal, ensuring compliance with legal regulations and institutional standards. While classifying data based on its sensitivity, organizations can determine appropriate handling procedures, which directly contribute to enhanced information security. For instance, sensitive student records require stricter handling protocols compared to less sensitive administrative data. Well-defined data handling processes not only facilitate compliance but also serve as a guideline for implementing security measures, thereby establishing a foundational layer of information security.

Lead City University Ibadan DO NOT COPY

2.3.2 Access Control and Information Security

Access control plays a vital role in safeguarding information systems, acting as the first barrier against unauthorized access. In educational institutions, models like Role-Based Access Control (RBAC) and Mandatory Access Control (MAC) are commonly applied. A study highlights that implementing RBAC in Oyo State-owned Polytechnics has improved

the management of user permissions. This ensures that access to sensitive data is restricted to authorized personnel based on their roles, thereby strengthening information security and operational efficiency[91]. This model aligns access rights with job roles, reducing the risk of data breaches. Additionally, integrating biometric and multi-factor authentication systems enhances access control by adding extra layers of verification, making unauthorized access more difficult.

According to a study, the adoption of biometric systems in polytechnics significantly reduces the potential for unauthorized access, enhancing the overall security of sensitive data[92]. Research shows that although implementing technologies like biometric and multi-factor authentication may involve initial costs, the long-term security benefits are significant. Information security awareness among Non-Academic Staff plays a crucial role in maintaining data integrity. Studies confirm that training and awareness programs help staff understand and follow data handling and access control protocols. In Oyo State-owned Polytechnics, one study found that regular training sessions on information security practices led to noticeable improvements in staff compliance and overall system security[93]. This highlights the necessity of fostering a culture of security awareness, where staff members are equipped to recognize potential security threats and adhere to established protocols effectively.

A scholar conducted a theoretical study to identify the status quo of risks and threats in information security[94]. The researchers examined the theoretical, material, and legislative dimensions of information security at both national and international levels. Their study concluded that the digital environment poses significant risks to information security, and that existing legislation is weak in addressing these threats. Separately, a scholar conducted a theoretical study to assess the current state of information security and transparency within

Lead City University Ibadan DO NOT COPY

the framework of electronic government[95]. The study addressed the natural security needs of information systems and explored additional dimensions of information security. It outlined standards for both security and transparency, along with implementation methods. Key recommendations included establishing political, regulatory, and legal frameworks to address security risks, developing policies tailored to e-government programs, and promoting awareness of the importance of protecting information systems.

In a study that aimed to identify the opinions of staff working in civil service authorities in Jordan regarding the difficulties facing the application of electronic services[96]. The study surveyed 413 randomly selected public officials to identify challenges in applying electronic services in Jordan. Key difficulties included management, financial resources, legislation and regulatory policies, information security and confidentiality, social awareness, and infrastructure. Management was seen as the most pressing issue. The study found no significant differences in responses based on gender, academic qualification, or experience, but did find differences related to age and nature of work. It recommended strengthening human and administrative resources and enhancing infrastructure and legislative frameworks for electronic services.

A scholar conducted a descriptive and analytical study to examine the ISO/IEC 27002 standard for managing information security systems. The study aimed to identify the policies and trends outlined in the standard and assess how well top Arab universities adhere to its guidelines[97]. The study used a descriptive method and content analysis, focusing on the top 20 Arab universities ranked by Webometrics. It found that all universities applied 11 basic ISO standards for managing information security systems. King Abdulaziz University ranked highest with 71.43% compliance, followed by King Fahd University (58.65%), Umm Al-Qura University (52.62%), and the University of Jordan (51.88%). However, 80.95% of the

Lead City University Ibadan DO NOT COPY

universities did not meet 50% of the sub-standards. The study recommended developing clear information security policies, assigning responsibilities to university units, providing advanced training, and ensuring regular data backups.

In another related line of research, the authors propose a critically-aware access control model for ubiquitous applications and smart environments[97]. The proposed framework relies on assigning user roles based on responsibilities and context, using two access control models, normal and critical-aware, activated depending on the situation's urgency. While the promote role function elevates privileges during emergencies, the framework lacks clarity on who should receive elevated access and when it should be granted. For example, in an emergency involving a bronchitis patient, only nurses specialized in respiratory care should access the medical records. However, the framework's reliance solely on general role and context fails to ensure that specific expertise is considered. This limitation could lead to inappropriate access or delays in care, highlighting the need for more granular control mechanisms that factor in qualifications, specialization, and real-time decision authority during critical scenarios.

Access control mechanisms are essential for enforcing organizational data handling. While regulating access based on predefined roles and criteria, they help prevent unauthorized access and reduce the risk of data breaches. Systems like Role-Based Access Control (RBAC) and Mandatory Access Control (MAC) function effectively when guided by clear, comprehensive data handling processes that define who should access what, and under which conditions. For instance, when a data handling stages restricts access to confidential student records to specific staff members, the access control system must enforce these limits precisely. In doing so, access control becomes the operational arm of data handling policies,

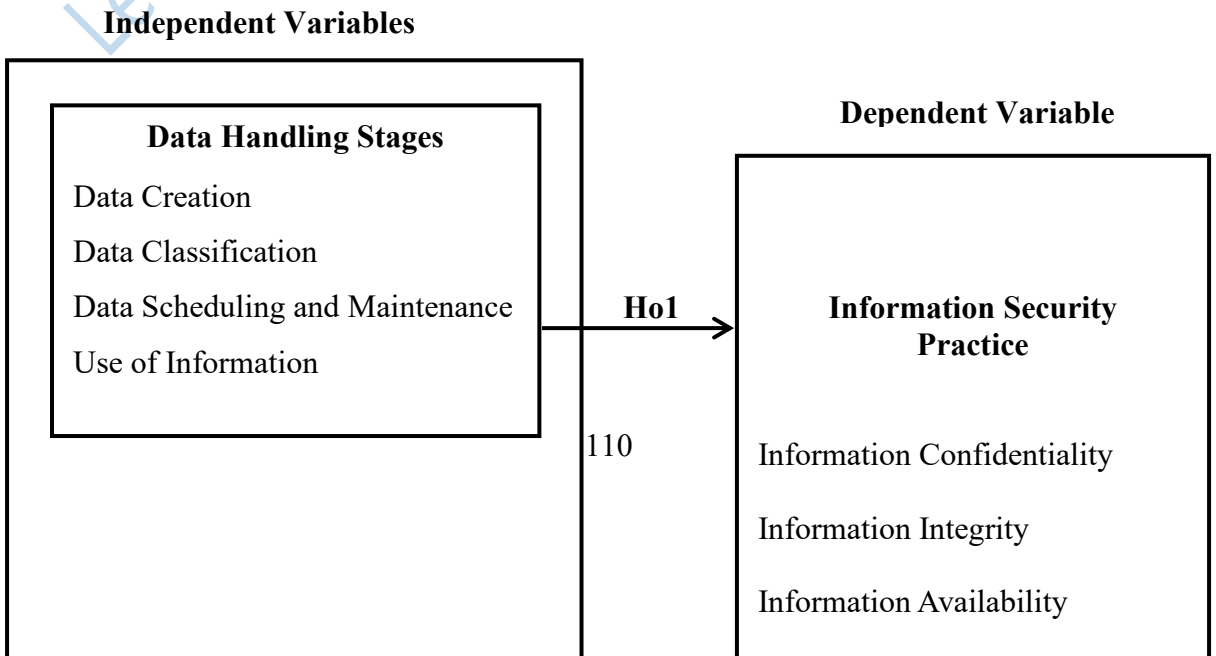
Lead City University Ibadan DO NOT COPY

translating policy guidelines into actionable safeguards that protect sensitive information from unauthorized access[98].

Despite advancements in data handling and access control, several persistent challenges continue to hinder effective information security. These include limited funding for security infrastructure, staff resistance to adopting new protocols, and the constantly evolving landscape of cyber threats. Research highlights that overcoming these obstacles requires strong institutional leadership that prioritizes strategic investment in information security systems, staff training, and adaptive technologies. Without this commitment, organizations risk falling behind in safeguarding sensitive data and maintaining regulatory compliance[99]. Establishing a dedicated information security governance framework strengthens accountability and ensures that security protocols evolve with emerging threats. Empirical evidence from Oyo State-owned Polytechnics highlights the importance of well-defined data handling policies, effective access control, and consistent security awareness among Non-Academic Staff.

Lead City University Ibadan DO NOT COPY

2.4 Conceptual Model



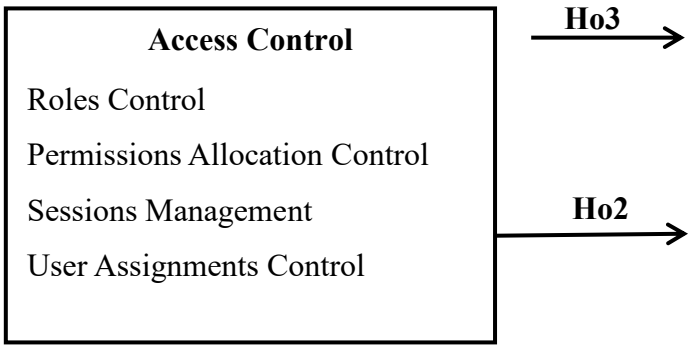


Figure 2.1: Conceptual Model of Information Security Data Handling Stages, and Access Control

Source: Researcher's Conceptual Model, 2024

According to the conceptual model of the study in figure 2.1 above, the dependent variable of this study is information security with three measures which are information confidentiality, information integrity and information availability as adopted from Triad CIA Model. The independent variables are data handling stages and access control[69]. The measures for data handling stages are data creation, data classification, data scheduling and maintenance and use of information[70,71,72]. While the measures for access control are roles definition, permissions allocation control, session management and user assignments control[73]. In the first hypothesis, the measures of data handling stages are to be tested on those of information security as depicted above, while in the second hypothesis, it indicates how measures of access control will be tested on those of information security. Lastly, in the third hypothesis, the combine influence of the two independent variables (data handling stages and access control) will be tested on the dependent variable (information security).

2.5 Summary of the Reviewed Literature

Existing literature on data handling, access control, and information security among Non-Academic Staff in Oyo State-owned Polytechnics shows notable gaps. Although these topics are studied across various sectors in this local context, research specific is limited, hindering

Lead City University Ibadan DO NOT COPY

insight into its unique challenges. Moreover, many studies depend on theoretical models rather than empirical evidence from staff, underscoring the need for both quantitative and qualitative research that reflects their real-world experiences and perspectives. Also, a few studies offer a holistic view of how data handling stages, access control, and information security practices work together within polytechnic settings. Most research treats these areas independently interconnected role, overlooking their security framework in forming a unified. Research on training programs for Non-Academic Staff is still limited, with many studies overlooking the crucial impact and education on of staff awareness information security. This gap highlights the need for targeted training initiatives that not only build technical skills but also foster a deeper understanding of security practices among personnel.

Another notable gap is the limited research on how emerging technologies like biometric systems and cloud computing affect data handling and access control in polytechnics. Existing studies rarely examine how these innovations reshape security protocols or influence adherence to regulatory standards. In addition, although some studies address challenges in implementing data handling policies and access control, few examine the specific obstacles faced by Non-Academic Staff. Key issues such as institutional resistance, limited funding, and inadequate resource allocation remain underexplored, leaving a gap in understanding the practical barriers implementation to effective security.

Existing literature offers limited insight into how Non-Academic Staff comply with national and international data protection laws. This gap points to the need for further research on how regulations like Nigeria's NDPR and global standards influence local practices within polytechnic institutions. Finally, most current studies are cross-sectional, offering only a limited view of present conditions. Longitudinal research is needed to capture how data

Lead City University Ibadan DO NOT COPY

handling, access control, and information security practices evolve over time, providing deeper insight into trends and long-term effectiveness.

The literature reviewed in this study consistently underscores the centrality of information security as a foundation for organizational effectiveness, with higher education institutions being no exception. Information security is understood not merely as a technological safeguard but as an integrated system of policies, processes, and cultural practices that collectively ensure the confidentiality, integrity, and availability of information. These three principles, articulated in the CIA triad, form the universal benchmark for evaluating information protection strategies. Confidentiality guarantees that only authorized persons have access to sensitive information, integrity ensures that data remains accurate and reliable, and availability provides for timely access to information when needed. Scholars also extend these principles to include authenticity, accountability, and reliability, thereby broadening the framework to address contemporary threats in dynamic digital environments.

In developed contexts, institutions have embedded these principles in comprehensive frameworks such as ISO/IEC 27001, the NIST Cybersecurity Framework, and the European Union' s GDPR. These systems institutionalize policies and compliance mechanisms, ensuring not only that sensitive records are technically protected but also that employees are trained and accountable. Higher education institutions in Europe and North America illustrate the benefits of such structured frameworks, with reductions in breaches, better accountability, and improved trust among stakeholders. Conversely, literature addressing Nigerian institutions reveals structural and managerial weaknesses that compromise the effective adoption of similar frameworks. Challenges include inadequate funding, poor infrastructure, weak enforcement of policies, and insufficient training of staff. Polytechnics, in particular, remain vulnerable because Non-Academic Staff handle large volumes of sensitive data,

Lead City University Ibadan DO NOT COPY

including admission records, student results, and transcripts, yet often operate in environments with weak security practices and hybrid record systems that combine manual and digital processes.

A growing body of research emphasizes the human dimension of information security. Breaches are frequently the result of insider actions, whether negligent or intentional, with studies suggesting that insider threats account for a majority of institutional vulnerabilities. Staff behavior, poor awareness, and the absence of security culture often outweigh purely technical concerns. This emphasis on culture and behavior is particularly relevant in Nigerian polytechnics, where empirical studies reveal widespread practices such as password sharing, improper storage of records, and weak adherence to confidentiality principles. The literature therefore points to the importance of security-aware cultures where staff not only know but internalize the value of confidentiality, integrity, and availability in daily operations.

Data handling stages are closely connected to information security because they describe the lifecycle of records from creation to final use. Data creation is the first stage, and literature stresses that errors introduced during this stage often persist throughout the record' s life, leading to long-term inefficiencies. In academic contexts, examples include errors in student registration or duplication of admission entries, which compromise the accuracy of institutional records. The classification stage requires sorting data according to sensitivity and purpose, but Nigerian institutions frequently lack formal classification frameworks, leaving highly sensitive data exposed. Maintenance and scheduling are equally critical, ensuring that records are updated, accurate, and systematically backed up. Failures in this stage contribute to delays in transcript issuance, poor reporting, and loss of institutional memory. The final stage, use of information, involves decision-making, planning, and communication. The

Lead City University Ibadan. DO NOT COPY

inability of institutions to retrieve and use reliable data on time undermines both operational efficiency and credibility.

The theoretical Records Continuum Model is often cited in this regard because it presents data handling not as discrete phases but as a continuous stewardship process. Data must be actively managed to preserve institutional evidence and support decision-making into the future. Nigerian polytechnics, however, frequently adopt a reactive approach, storing information without standardized policies or long-term strategies, which results in inefficiency and vulnerability to breaches. Weak integration of technology into data handling exacerbates these challenges. While many institutions worldwide use digital records management systems and cloud platforms to improve efficiency and reliability, Nigerian polytechnics continue to rely on hybrid systems that expose them to duplication, data loss, and insider manipulation.

Access control mechanisms, another key focus of the literature, provide the structural means by which confidentiality is enforced. Historically, discretionary and mandatory access control models shaped security practices. Discretionary access gave data owners' decision-making authority, which, while flexible, was inconsistent and vulnerable to misuse. Mandatory access was more rigorous, using classification levels to enforce restrictions, but it proved too rigid for dynamic environments such as academic institutions. The development of role-based access control (RBAC) addressed many of these limitations by tying permissions to organizational roles rather than to individuals. This model simplifies management, ensures consistency, and limits privilege creep, making it particularly suitable for institutions with hierarchical structures such as polytechnics.

Empirical research supports the effectiveness of RBAC in curbing insider threats, which are a persistent concern in educational institutions. RBAC reduces opportunities for insider misuse

Lead City University Ibadan DO NOT COPY

by limiting access strictly according to job function. However, challenges remain in contexts where institutional roles are not clearly defined or where informal cultural practices undermine compliance. Nigerian polytechnics provide such examples, with Non-Academic Staff often given broad, poorly monitored access to sensitive data and engaging in practices such as credential sharing. Recent innovations in access control, such as attribute-based and risk-adaptive models, have been proposed as more flexible alternatives, yet their complexity and infrastructure requirements limit their applicability in Nigerian contexts. RBAC therefore remains the most feasible option, but its adoption is hindered by infrastructural constraints, role ambiguity, and weak institutional culture.

Theoretical frameworks provide additional lenses for interpreting these issues. The CIA triad highlights the goals of confidentiality, integrity, and availability, and aligns directly with the processes of access control and data handling. Confidentiality is threatened by weak controls, integrity is undermined by poor data maintenance, and availability suffers when scheduling and retrieval systems are inefficient. The Records Continuum Model emphasizes the lifecycle perspective, urging institutions to treat records as dynamic resources requiring continuous stewardship rather than static repositories of information. RBAC theory operationalizes these goals by ensuring that access is structured, consistent, and tied to organizational functions rather than to personal discretion. Together, these theories provide a robust framework for analyzing information security practices. However, the literature notes a significant implementation gap in Nigerian institutions. Policies exist but are often not enforced, record stewardship remains reactive, and RBAC is poorly institutionalized due to infrastructural and cultural challenges.

Empirical studies further illuminate the divergence between theory and practice. While institutions in developed contexts demonstrate the value of integrated frameworks, Nigerian

Lead City University Ibadan DO NOT COPY

polytechnics struggle with inconsistent enforcement, limited awareness, and resource constraints. Research shows that Non-Academic Staff frequently lack training in information security, contributing to breaches and inefficiencies. Insider threats remain a recurring theme, as credential sharing, weak authentication, and informal practices undermine security. Moreover, most Nigerian studies are cross-sectional, focusing on immediate challenges such as delays in issuing results or poor digitization, with few longitudinal assessments of how interventions affect long-term outcomes. This gap limits the ability of policymakers to design sustainable reforms. Comparative research within Africa is also limited, reducing opportunities for benchmarking and learning from regional peers.

The conceptual model guiding this study integrates insights from the CIA triad, the Records Continuum Model, and RBAC theory, positioning data handling and access control as interdependent processes that determine the effectiveness of information security in registry departments. Data handling ensures the accuracy and availability of records, while access control secures their confidentiality. Without effective data handling, access controls lose their value because unreliable records cannot support institutional decision-making. Similarly, without robust access control, data handling processes become vulnerable to unauthorized manipulation. The framework also highlights the contextual realities of Nigerian polytechnics, where infrastructural weaknesses, informal work cultures, and inadequate enforcement complicate the adoption of best practices. This integrated conceptual lens provides a means of analyzing current practices and designing tailored interventions.

The reviewed literature concludes by affirming the importance of information security in higher education institutions while also revealing critical gaps that justify further investigation. The gaps include limited adoption of global best practices, weak integration of theoretical models into local practice, inadequate attention to cultural and behavioral

Lead City University Ibadan DO NOT COPY

dimensions, and a lack of longitudinal and comparative empirical studies. Nigerian polytechnics, in particular, are characterized by poor infrastructure, weak training, and hybrid record systems that expose them to breaches and inefficiencies. Non-Academic Staff, as custodians of sensitive records, are central to the problem yet remain underexplored in the literature. By focusing on their roles and practices, this study addresses a vital gap and contributes to both academic knowledge and practical policy reforms.

Lead City University Ibadan DO NOT COPY

Endnotes

1. S. Aathilakshmi, A. Prasanth, K. K. Sowndarya & P. C. Thắng. “Access Control Using AI Based Biometric Systems”, **Case Study**. 2024, 156–171. https://doi.org/10.1201/9781032702377-9

2. A. Afshar. “*Authentication, Authorization, and Selective Disclosure for IoT Data Sharing Using Verifiable Credentials and Zero-Knowledge Proofs.”* **Lecture Notes in Computer Science**, 2023, 88–101. https://doi.org/10.1007/978-3-031-25467-3_6

3. O. Aladesanmi, B. Afolabi & T. O. Oyebisi. “Assessing Network Services and Security in Nigeria Universities” **JCSIA**. 19(1), 2012, 60–66. https://doi.org/10.4314/JCSIA.V19I1.8

4. A. I. Awad, A. Babu, E. Barka & K. Shuaib. *“AI-Powered Biometrics for Internet of Things Security: A Review and Future Vision”*. **Journal of Information Security and Applications**, 2024. https://doi.org/10.1016/j.jisa.2024.103748

5. B. Badamasi & S. C. A. Utulu. “*Framework for Managing Cybercrime Risks in Nigerian Universities. arXiv:*” **Computers and Society**. 2021. https://dblp.uni-trier.de/db/journals/corr/corr2108.html#abs-2108-09754

6. S. S. Bakare, .A. O. Adeniyi, C. U. Akpuokwe & N. E. Eneh. *“Data Privacy Laws and Compliance”*: **A Comparative Review of the EU GDPR and USA Regulations**, 2024. https://doi.org/10.51594/csitrj.v5i3.859

7. D. U. Bille, “*Impact of Cyberspace on the Cybersecurity of Critical National Assets Infrastructures in Nigeria: A Review of Education and Financial Sectors.”* **World Journal Of Cybersecurity**, 2022.

8. Advanced Research and Reviews, 16(1), 2022, 595–604. https://doi.org/10.30574/wjarr.2022.16.1.1057

9. S. Boopathi. *“Securing Healthcare Systems Integrated With IoT”*, **IGI Global**, 2023, 186 - 209.

10. E. Michael, Whitman & J. Herbert. “*Principles of Information Security*”, 6, 2009

11. C. El Filali, I. Bourian & K. Chougdali. “*Privacy-Preserving And Access Control Scheme For IoT-Based*” **Healthcare Systems Using Ethereum Blockchain.** 2024,1-6. https://doi.org/10.1109/commnet63022.2024.10793370

12. E. S. Essien & E. Egbeji. “*Digitalizing Cyber Security for Data Management in Higher Education Implication for Educational Management in Nigeria”*. **Journal of Advances in Education and Philosophy**, 2024. https://doi.org/10.36348/jaep.2024.v08i04.001

13. X. Fan, X. Wei, Q. Zhao, B. Jin, Y. Zheng, Z. Zha, D. Xiao, L. Feng, G. Wu & J. Hu. “*Exploration on the Application of Multimodal Biometric Feature Recognition in System Access Control*”, 2024. https://doi.org/10.1109/csnt60213.2024.10545831

Lead City University Ibadan DO NOT COPY

14. M. Farhan, A. Salih & U. Butt. "*Enhancing Secure Access and Authorization in Healthcare IoT through an Innovative Framework: Integrating OAuth"*, **DIDs, and VCs**. 2023, 254–261. https://doi.org/10.1145/3625156.3625193

15. S. Farouk, C. Uppin & G. George. "*Enhancing Cybersecurity in Nigeria: A Proposed Risk Management Framework for Universities"*, 2024, 1–8. https://doi.org/10.1109/seb4sdg60871.2024.10629748

16. V. Garg. "*Modern Data Governance Technologies and Their Role in Regulatory Compliance: A Study on GDPR and HIPAA*". **International Scientific Journal of Engineering and Management**, 03(12), 2024, 1–6. https://doi.org/10.55041/isjem0276

17. **International Comparative Legal Guides (ICLG).** *Data Protection Laws and Regulations: Nigeria*, 2024, 2024–2025. https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria#:~:text=The%20Nigeria%20Data%20Protection%20Commission%20%28%E2%80%9CNDPC%E2%80%9D%29%20is%20the,NDPA%20in%20Nigeria.%20The%20NDPA%20establishes%20the%20NDPC

18. S. Kumar. *"Biometric Systems Security and Privacy Issues."* 2024, 68–91. https://doi.org/10.1201/9781032614663-4

19. J. Laksito, B. Pratiwi & W. Ariani. "*Harmonizing Data Privacy Frameworks in Artificial Intelligence: Comparative Insights from Asia and Europe*." **Perkara**, 2(4), 2025, 579–588. https://doi.org/10.51903/perkara.v2i4.2229

20. A. Naboth-Odums, F. E. Abanyam, A. Abdulkadir, & V. A. Abanyam. "*Information and Security Control Mechanisms Embraced for Effective Information Management in Colleges of Education in Nigeria."* **Golden Ratio of Social Science and Education**, 2(2), 2022, 98–111. https://doi.org/10.52970/grsse.v2i2.183

21. D. O. Njoku, E. C. Nwokorie, S. A. Okolie & J. N. Odii. "*Cyberspace Activities Awareness and Security Strategies in Tertiary Institutions in Nigeria."* 3(2), 2019, 439–445. https://irejournals.com/formatedpaper/1701507.pdf

22. N. D. Nte, V. A. Teru, & A. Ridwan. "*Challenges of Information Security Laws and Legislations in Nigeria's Institutions of Higher Education: Views from Yola, Adamawa State."* **Research and Development in Education**, 4(2), 2024, 1498–1519. https://doi.org/10.22219/raden.v4i2.35711

23. B. C. Oguguo & C. A. Ocheni. "Cybersecurity: a Tool for Curbing Examination Breaches and Improvement of the Quality of Large-Scale Educational Assessments." **Information Security Journal: A Global Perspective,** 2023, 1–15. https://doi.org/10.1080/19393555.2023.2284761

24. K. O. Okokpujie, C. G. Kennedy, K. Nnodu & E. Noma-Osaghae. "*Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe*

Good City University Ibadan DO NOT COPY

Email Usage in Academic Environment (A Case Study of a Nigerian Leading University).” **International Journal of Sustainable Development and Planning,** 18(1), 2023, 255–263. https://doi.org/10.18280/ijsdp.180127

25. B. D. Oladokun, E. Oloniruha, D. Mazah & O. Okechukwu. “*Cybersecurity Risks in Libraries: Why Universities Libraries in African Need to Promote Cyberethical Practices*”, 2024. https://doi.org/10.25159/3005-4222/15320

26. A. Raymond. “*Data Management Regulation: Your Company Needs an Up-to-Date Data/Information Management Policy.”* **Social Science Research Network**, 2013. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265560

27. V. K. A. Seshagirirao & A. B. Babatope. *“Data Privacy, Security, and Governance: A Global Comparative Analysis of Regulatory Compliance and Technological Innovation.”* **Global Journal of Engineering and Technology Advances,** 21(3), 2024, 190–202. https://doi.org/10.30574/gjeta.2024.21.3.0246

28. W. F. Shah. *“Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA.”* **International Journal for Research in Applied Science and Engineering Technology**. 2023. https://doi.org/10.22214/ijraset.2023.55551

29. R. Trabelsi, G. Fersi & M. Jmaiel. *“Access Control in Internet of Things”*: **A Survey**, 2023. https://doi.org/10.1016/j.cose.2023.103472

30. A. Wahid Abdul Wahab & M. Y. Idna Idris. *“Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions.”* **Applied Sciences**, 2023. https://doi.org/10.3390/app13148048

31. K. Barata, R. Bennett, P. Cain, & D. Routledge. *“From Accounting to Accountability: Managing Financial Records as a Strategic Resource”.* **Namibia a case study. London: IRMT**, 2001.

32. M. Bradford & J. Florin. “*Examining the Role of Innovation Diffusion Factors on the Implementation Success of Enterprise Resource Planning Systems*”. **International Journal of Accounting Information Systems**, 4 (3), 2003, 205-225.

33. GAO. *“Information Management: Challenges in Managing and Preserving Electronic Records.”* **Report to Congress Requesters**; 2002, GAO, USA

34. A. Griffin & P. Mazikana. *“Fostering Trust and Transparency in Governance: Investigating and Addressing the Requirements for Building Integrity in Public Sector Information Systems in the ICT Environment.”* **IRMT, London**, 2007.

35. M. Hoyle & J. Wamukoya. *“Transparency in Governance: Addressing the Requirements for Building Integrity in Public Sector Information Systems in the ICT Environment.”* **IRMT, London**, 2006

36. IRMT. *“Managing Personnel Records in an Electronic Environment: TERM Project”*,

Lead City University Ibadan DO NOT COPY

IRMT, London, 2009 https://www.irmt.org

37. H. Kemoni. "*Theoretical Framework and Literature Review in Graduate Records Management Research*". **African Journal of Library, Archives and Information Sciences.** 18 (2), 2008, 103-117

38. H. Kemoni & P. Ngulube "*Relationship between Records Management, Public Service Delivery and Attainment of United Nations Millennium Development Goals in Kenya*". **Paper presented at the XIX Bi-Annual ESARBICA General Conference, Dare es Salaam Tanzania** 2007, 18-22

39. M. Makhura & A. Du Toit. "*Records Management and Information User behavior at SANParks: A Case Study*". **Mousaion** 23(2): 2007, 213-229

40. M. T. Manyambula. "*Records Management and Accountability.*" **Paper Presented at the XIX Bi-Annual ESARBICA General Conference, Dare Es Salaam Tanzania** 2007 18-22

41. N. Mnjama, & J. Wamukoya. *"E-Government and Records Management: An Assessment Tool for E-records Readiness in Government."* **Paper Presented at the SADC Workshop on E-Government, Gaborone** 2004, 14- 16.

42. L. Sejane, *"Records Management in Africa: Three Case Studies and a Proposal. In Information 2000: A Version for the SCECSAL Region."* **Proceedings of the 14th Conference of Eastern, Central and Southern African Libraries**, 2000, 10-15

43. S. Mutula. "*Evolving Paradigm in the Networked World and their Implication for Information Management in African Libraries*". **African Journal of Library, Archives and Information Sciences.** 18 (2), 2008, 89-102

44. M. Tomar, & Jawaharbabu Jeyaraman. "*Reference Data Management: A Cornerstone of Financial Data Integrity.*" **Journal of Knowledge Learning and Science Technology** ISSN 2959-6386 (online). 2(1), 2023, 137–144. https://doi.org/10.60087/jklst.vol2.n1.p 144.

45. K. Clark. *"Yahoo Lawsuit Alleges Employee Stole Trade Secrets upon Receiving Trade Desk Job Offer"*. **The Drum**; 2022. https://www.thedrum.com/news/2 022/05/19/yahoo-lawsuit-allegesemployee-stole-trade-secrets-uponreceiving-trade-desk-job

46. H. Omotunde & M. Ahmed. *"A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond."* **Mesopotamian Journal of Cyber Security**. 2023, 115–133. https://doi.org/10.58496/MJCSC/2023/ 016

47. N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, P. Burnap. *"Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses."* **Electronics**. 9(9), 2020, 1460. https://doi.org/10.3390/electronics909

48. S. T. Alshammari, A. Albeshri & K. Alsubhi. *"Integrating a High-Reliability Multicriteria Trust Evaluation Model with Task Role-Based Access Control For Cloud Services."*

Lead City University Ibadan DO NOT COPY

Symmetry. Mar. 13(3), 2021, 492. https://doi.org/10.3390/sym13030492

49. P. Paganini. "*Block Discloses Data Breach Involving Cash App Potentially Impacting 8.2 Million US Customers*." **Security Affairs**; 2022. https://securityaffairs.com/12989 2/data-breach/block-cash-app-databreach.html

50. C. Glover. "*Pegasus Airline Breach Sees 6.5TB of Data Left in Unsecured AWS Bucket.*" **Tech Monitor;** 2022. https://techmonitor.ai/technology/cybersecurity/pegasus-airline-data-breachaws-bucket

51. A. K. Malik et al. "*From Conventional to State of-the-Art IOT Access Control Models*." **Electronics.** 9(10), 2020, 1693. https://doi.org/10.3390/electronics9101693

52. R. A. Teimoor. "*A Review of Database Security Concepts, Risks, and Problems*." **UHD Journal of Science and Technology**. 5(2), 2021, 38–46. https://doi.org/10.21928/uhdjst.v5n2y2 021 pp38-46

53. A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi & S. A. Ajayi. *"Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale."* **Asian Journal of Research in Computer Science.** 17(5), 2024, 85–107. https://doi.org/10.9734/ajrcos/2024/v1 7i5441.

54. S. Prabhu & N. Thompson. "*A Primer on Insider Threats in Cybersecurity."* **Information Security Journal: A Global Perspective.** 31(5), 2021, 1–10. https://doi.org/10.1080/19393555.202 1.1971802

55. R. A. Alsowail, & T. Al-Shehari. "*Empirical Detection Techniques of Insider Threat Incidents."* **IEEE Access**, 8, 2020, 78385– 78402.

56. N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye & C. S. Adigwe. "*Evolving Access Control Paradigms*": **A Comprehensive Multidimensional Analysis of Security Risks and System Assurance in Cyber Engineering**. 17(5), 2024, 108–124. https://doi.org/10.9734/ajrcos/2024/v1 7i5442

57. A. Djenna, S. Harous & D. E. Saidouni. "*Internet of Things Meet the Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure.*" **Applied Sciences.** 11(10), 2021, 4580. https://doi.org/10.3390/app11104580

58. M. N. Al-Mhiqani et al. "*A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations."* **Applied Sciences**. 10(15), 2020, 5208. https://doi.org/10.3390/app10155208

59. Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi & S. S. Ajayi. *"Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend."* **Asian Journal of Advanced Research and Reports.** 18(1), 2024, 30–35. https://doi.org/10.9734/ajarr/2024/v18i 1596

60. J. Y. Li, R. Sun, W. Tao & Y. Lee. *"Employee Coping with Organizational Change in the Face of a Pandemic: The Role of Transparent Internal Communication."* **Public**

Lead City University Ibadan DO NOT COPY

Relations Review. 47(1), 2021, 101984. https://doi.org/10.1016/j.pubrev.2020. 101984

61. K. Albulayhi, A. Abuhussein, F. Alsubaei, & F. T. Sheldon. "*Fine-Grained Access Control in the era of Cloud Computing: An Analytical Review*." **10th Annual Computing and Communication Workshop and Conference (CCWC);** 2020 https://doi.org/10.1109/ccwc47524.20 20.9031179

62. M. Pundlik & P. P. Jadhav. "Block chain technology in healthcare system for sharing confidential information between departments and doctors." **International Journal of Intelligent Systems and Applications in Engineering.** 12(12s), 2024 01-10. https://ijisae.org/index.php/IJISA E/article/view/4488

63. S. Parkinson, S. Khan. *"A Survey on Empirical Security Analysis of Access Control Systems: A Real-World Perspective."* **ACM Computing Surveys**; 2022. https://doi.org/10.1145/3533703

64. K. R. Rao, A. Nayak & I. G. Ray. Rahulamathavan Y, Rajarajan M. "*Role Recommender-RBAC: Optimizing User-Role Assignments in RBAC*." **Computer Communications**. 166, 2021, 140–153. https://doi.org/10.1016/j.comcom.2021 .12.006

65. J. Park, R. Sandhu, M. Gupta & S. Bhatt. "*Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems.*" **IEEE Access**. 9, 2021; 151004–151022. https://doi.org/10.1109/access.2021.3 126201

66. S. Pal, & Z. Jadidi. "*Protocol-Based and Hybrid Access Control for the IOT: Approaches and Research Opportunities."* **Sensors**. 21(20), 2021, 6832. https://doi.org/10.3390/s21206832

67. G. Nyame & Z. Qin. *"Precursors of Role-Based Access Control Design in KMS: A Conceptual Framework."* **Information**. 11(6), 2020, 334. https://doi.org/10.3390/info11060334

68. S. Ameer, J. Benson & R. Sandhu. "*An Attribute-Based Approach Toward a Secured Smart-Home IOT Access Control and a Comparison with a Role-Based Approach*." **Information**. 13(2), 2022; 60. https://doi.org/10.3390/info13020060

69. R. El Sibai, N. Gemayel, J. Bou Abdo & J. Demerjian. "*A Survey on Access Control Mechanisms for Cloud Computing*." **Transactions on Emerging Telecommunications** Technologies. 31(2), 2019 https://doi.org/10.1002/ett.3720

70. S.J.A. Flynn, (2001) "*The Records Continuum Model in Context and its Implications for Archival Practice*", **Journal of the Society of Archivists** 22(1), 2001, 79-93.

71. P. Marshall, "*Life Cycle Versus Continuum: What is the Difference?*" **Informaa Quarterly, Records Management Association of Australia, Sydney**, 16(2), 2000, pp.20-25.

72. T. Zaidi, M. Usman, M. Umar Aftab, H. Aljuaid & Y. Yasin Ghadi. "*Fabrication of*

Lead City University Ibadan DO NOT COPY

flexible Role-Based Access Control Based on Block Chain for Internet of Things Use Cases." **ieeexplore.ieee.org;** 2023.

73. Computer Security Division. "*Role Engineering and RBAC Standards - Role Based Access Control, CSRC, NIST"*; 2016. https://csrc.nist.gov/projects/rolebased-access-control/role-engineeringand-rbac-standards

74. R. A. Alsowail & T. Al-Shehari. "*A Multi-Tiered Framework for Insider Threat Prevention.*" **Electronics**. 10(9), 2021, 1005. https://doi.org/10.3390/electronics100 91005

75. B. Yang. "*Enforcement of Separation of Duty Constraints in Attribute-Based Access Control*." **Computers and Security**. 131, 2023, 103294. https://doi.org/10.1016/j.cose.2023.10 3294

76. K. Ragothaman, Y. Wang, B. Rimal & M. Lawrence. "*Access Control for IOT: A Survey of Existing Research, Dynamic Policies, and Future Directions*." **Sensors**. 23(4), 2023, 1805. https://doi.org/10.3390/s23041805

77. A. Chiquito, U. Bodin, & O. Schelen. "*Attribute Based Approaches for Secure Data Sharing in Industrial Contexts*." **IEEE Access**. 11, 2023, 10180–10195. https://doi.org/10.1109/access.2023.3 240000

78. S. Ahmadi. "*Zero Trust Architecture in Cloud Networks: Application, Challenges, and Future Opportunities.*" **Journal of Engineering Research and Reports**. 26(2), 2024, 215–228. https://doi.org/10.9734/jerr/2024/v26i2 1083

79. S. Aboukadri, A. Ouaddah, & A. Mezrioui. "*Machine Learning in Identity and Access Management Systems: Survey and Deep Dive*." **Computers and Security**. 139, 2024:103729. https://doi.org/10.1016/j.cose.2024.10 3729

80. S. O. Olabanji. "*AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems*." **Asian Journal of Research in Computer Science.** 17(3), 2024, 38–56. https://doi.org/10.9734/ajrcos/2024/v1 7i3423

81. K. Putch. "*Healthcare Security Services Firms Tackle Ransomware Spike*," **TechTarget. IT Channel,** 2021. https://www.techtarget.com/searc hitchannel/feature/Healthcare-securityservices-firms-tackle-ransomwarespike?bucket=NEWS&topic=299987

82. S. Deng et al. "*Cloud-Native Computing: A Survey from the Perspective of Services*." **Proceedings of the IEEE.** 112(1), 2024, 12–46. https://doi.org/10.1109/JPROC.2024.3 353855

83. T. Baumer, M. Müller & Günther Pernul. "*System for Cross-Domain Identity Management (SCIM): Survey and Enhancement with RBAC*." **IEEE Access**. 11, 2023, 86872–86894. https://doi.org/10.1109/access.2023.3 304270

84. U. Rauf, M. Shehab, N. Qamar & S. Sameen. "*Formal Approach to Thwart Against*

Lead City University, Ibadan DO NOT COPY

Insider Attacks: A Bio-Inspired Auto-Resilient Policy Regulation Framework." **Future Generation Computer Systems.** 117, 2021, 412–425. https://doi.org/10.1016/j.future.2020.1 1.009

85. K. R. Dodiya, M. Jha, & S. Jha. "*Fortifying the Digital Forge: Unleashing Cybersecurity in the Interconnected World of Digital Manufacturing* 2024 https://www.igiglobal.com/chapter/fortifying-the-digitalforge/336132

86. M. A. Azad, J. Arshad, S. Mahmoud, K. Salah & M. Imran. "*A privacy-preserving Framework for Smart Context-Aware Healthcare Applications."* **Transactions on Emerging Telecommunications Technologies**. 2019;e3634. https://doi.org/10.1002/ett.3634

87. A. S. M. Kayes et al. "*A Survey of Context Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues.*" **Sensors**. 20(9), 2020, 2464. https://doi.org/10.3390/s20092464

88. G. Taranto-Vera, P. Galindo-Villardón, J. Merchán-Sánchez-Jara, J. Salazar-Pozo, A. Moreno-Salazar, & V. Salazar-Villalva. *"Algorithms and Software for Data Mining and Machine Learning: A Critical Comparative View From a Systematic Review of the Literature."* **The Journal of Supercomputing.** 77(10), 2021, 11481–11513. https://doi.org/10.1007/s11227-021- 03708-5

89. K. Raza Nowrozy, H. Ahmed Wang & T. McIntosh. *"Towards a Universal Privacy Model for Electronic Health Record Systems: An Ontology and Machine Learning Approach."* **MDPI**. Jul. 10(3), 2023, 60–60. https://doi.org/10.3390/informatics100 30060

90. C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke & S. A. Ajayi. "*Forecasting the Future: the Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy.*" **Asian Journal of Economics, Business and Accounting**. 24(4), 2024, 126–146. https://doi.org/10.9734/ajeba/2024/v24 i41269

91. S. O. Olabanji. AI-driven cloud security: "*Examining the Impact of User Behavior Analysis on Threat Detection.*" **Asian Journal of Research in Computer Science.** 17(3), 2024, 57–74. https://doi.org/10.9734/ajrcos/2024/v1 7i3424

92. U. F. Eze, C. Etus & J. E. Uzukwu. *"Database System Concepts, Implementations and Organizations-A Detailed Survey."* **International Journal of Scientific Engineering and Research (IJSER)**. 2(2), 2014, 22–34.

93. S. A. Ajayi, O. O. Olaniyi, T. O. Oladoyinbo, N. D. Ajayi & F. G. Olaniyi. "*Sustainable Sourcing of Organic Skincare Ingredients: A Critical Analysis of Ethical Concerns and Environmental Implications."* **Asian Journal of Advanced Research and Reports**. 18(1), 2024, 65–91. https://doi.org/10.9734/ajarr/2024/v18i 1598

94. F. U. Quadri, O. O. Olaniyi & O. O. Olaoye. *"Interplay of Islam and Economic Growth: Unveiling the Long-Run Dynamics in Muslim and Non-Muslim Countries."* **Asian**

Leadership University Ibadan DO NOT COPY

Journal of Education and Social Studies. 49(4), 2023, 483–498. https://doi.org/10.9734/ajess/2023/v49 i41226

95. T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, & A. I. Alao. "*Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics.*" **Asian Journal of Advanced Research and Reports**. 18(2), 2024, 1–23. https://doi.org/10.9734/ajarr/2024/v18i 2601

96. O. O. Adebiyi, S. O. Olabanji, & O. O. Olaniyi. "*Promoting Inclusive Accounting Education Through the Integration of Stem Principles for a Diverse Classroom.*" **Asian Journal of Education and Social Studies**. 49(4), 2023, 152–171. https://doi.org/10.9734/ajess/2023/v49 i41196

97. O. O. Olaniyi, N. Shah, & N. Bahuguna. "*Quantitative Analysis and Comparative Review of Dividend Policy Dynamics within the Banking Sector: Insights from Global and U.S. Financial Data and Existing Literature.*" **Asian Journal of Economics, Business and Accounting**. 23(23), 2023, 179–199. https://doi.org/10.9734/ajeba/2023/v23 i231180

98. S. O. Olabanji, O. B. Oladoyinbo, C. U. Asonze, T. O. Oladoyinbo, S. A. Ajayi & O. O. Olaniyi. *"Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation.* **Asian Journal of Economics, Business and Accounting.** 24(4), 2024, 106–125. https://doi.org/10.9734/ajeba/2024/v24 i41268

99. S. O. Olabanji, T. O. Oladoyinbo, C. U. Asonze, C. S. Adigwe, O. J. Okunleye & O. O. Olaniyi. "*Leveraging Fintech Compliance to Mitigate Cryptocurrency Volatility for Secure US Employee Retirement Benefits: Bitcoin ETF Case Study*." **Asian Journal of Economics, Business and Accounting**. 24(4), 2024, 147–167.

Lead City University Ibadan DO NOT COPY

Chapter Three

Methodology

This chapter presents the methodology used in this study. The different sub-sections include research design, population of the study, sample and sampling technique, description of research instrument, validity of research instrument, reliability of research instrument, method of data collection, and method of data analysis.

3.1 Research Design

This study adopted a descriptive survey research design. This was considered useful for this study as it aims to accurately and systematically describe a population or phenomenon[1]. This method is appropriate because it was found useful in the collection of data on phenomena that cannot be directly observed and allows the researcher to compare responses from all respondent groups at the same time. The descriptive research design was considered suitable in carrying out the study as it tends to enable the researcher to determine the relation between Data handling Stages, Access Control, and Information Security Practice among Non-Academic Staff in Oyo State-owned Polytechnics.

3.2 Population of the Study

The population of this study consists of one thousand one hundred and nine (1109) Non-Academic Staff in Oyo States-owned Polytechnics, Nigeria, ranging from Administrative (Deputy Registrars, Principal Assistant Registrars, Senior Assistant Registrars and Assistant Registrars), Database Administrative, Executive (Chief Executive Officers, Principal Executive Officers, Senior Executive Officers, Executive Officers and Clerical Officers), Health Records Officers and Secretarial (Chief Confidential Secretaries, Confidential Secretaries and Secretarial Assistants) cadres. This implied that the population covered Non-Academic Staff of The Polytechnic, Ibadan, Adeseun Ogundoyin Polytechnic, Eruwa and

Lead City University Ibadan DO NOT COPY

The Oke-Ogun Polytechnic, Saki. These Polytechnics were selected because the perceived gaps which form the purpose of this study has been traced to exist there.

Table 3.1: Population of the Study

S/N	School	Population
1	The Polytechnic, Ibadan	494
2	Adeseun Ogundoyin Polytechnic, Eruwa	336
3	The Oke-Ogun Polytechnic, Saki	279
	Total	**1109**

Source:[2,3,4]

3.3 Sample Size and Sampling Technique

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, as shown in Table 3.2[5]. For this study, the stratified sampling technique was adopted, this stratified represent the total population from the actual population of the Non-Academic Staff in these institutions.

Table 3.2: Table for determining sample size of a known population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	354
35	32	150	108	360	186	**1100**	**285**	5000	357
40	36	160	113	380	191	1200	291	6000	302
45	40	170	118	400	196	1300	297	7000	364
50	44	180	123	420	201	1400	302	8000	367
55	48	190	127	440	205	1500	306	9000	368
60	52	200	132	460	210	1600	310	10000	370
65	56	210	136	480	214	1700	313	15000	375
70	59	220	140	500	217	1800	317	20000	377
75	63	230	144	550	226	1900	320	30000	379
80	66	240	148	600	234	2000	322	40000	380
85	70	250	152	650	242	2200	327	50000	381
90	73	260	155	700	248	2400	331	75000	382
95	76	270	159	750	254	2600	335	100000	384

Lead City University Ibadan DO NOT COPY

Source: Krejcie and Morgan (1970)[5] Sample Size Determinant

Table 3.3 Stratified Sampling Calculation for the Sample used

S/N	Name of Schools	% of total population	Calculated no for each sample
1.	The Polytechnic, Ibadan	$\frac{494}{1109}$ X 100 = 45%	$\frac{45 \text{ X } 285}{100}$ = 128
2.	Adeseun Ogundoyin Polytechnic, Eruwa	$\frac{336}{1109}$ X 100 = 30%	$\frac{30 \text{ X } 285}{100}$ = 86
3.	Oke–Ogun Polytechnic	$\frac{279}{1109}$ X 100 = 25%	$\frac{25 \text{ X } 285}{100}$ = 71
	Total	**100%**	**285**

Source: Researcher, 2025

3.4 Description of the Research Instrument(s)

The instrument used for this study was a structured questionnaire, which allowed the researcher to readily assess the structured questions and responses to meet the study's goal. The four-point Likert scale design was used in this study, which helps the researcher to give options for respondents to choose from. Data on the factors under study were collected using self-reported questionnaires. In this study, the Data Handling Stages, Access Control and Information Security (DHSACIS) scale was employed.

Section A: This section was used to collect demographic information from respondents, and it provides biographical information about respondents based on three factors: gender, age, level and year of experience.

Section B: Information Security scale indicated how secure the information of Oyo State-owned Polytechnics is. This scale used four-point Likert scale which are: Very High = 4, High = 3, Low = 2, Very Low= 1. This research instrument was adapted[6]. This section has three (3) sub-scales representing each measure for the variable with a total of fifteen (15)

Lead City University Ibadan DO NOT COPY

items. The first sub-scale was used to measure information confidentiality and it contains five (5) items. The second sub-scale was used to measure information integrity and it contains five (5) items. The third sub-scale was used to measure information availability and it consists of five (5) items. An example of these items is on "The security features, service levels, and management requirements of all network services have been identified and documented.

Section C: Data handling stages scale, which indicates the level at which respondents handle and process academic data. This scale used a four-point Likert scale, which is: Strongly Agree = 4, Agree = 3, Disagree = 2, and Strongly Disagree = 1. This research instrument was adapted[7]. This section has four (4) sub-scales representing each measure for the variable, with a total of twelve (12) items. The first sub-scale was used to measure data creation, and it contains three (3) items. The second sub-scale was used to measure data classification, and it contains three (3) items. The third sub-scale was used to measure data scheduling and maintenance; it also consists of three (3) items. The fourth sub-scale was used to measure the use of information, with three (3) items. Example of these items is "Planning the time it takes to organize and document the data, code, and other supporting files so that others can understand it".

Section D: Access Control scale, which reflects factors such as Roles Definition, Permissions Allocation Control, Session Management, and User Assignments Control. The scale is also of four-point Likert scale which are: Very High = 4, High = 3, Low = 2, Very Low= 1**.** This instrument was adapted[8.] This section has four (4) sub-scales representing each measure for the variable with a total of twelve (12) items. The first sub-scale was used to measure roles, and it contains three (3) items. The second sub-scale was used to measure permission and it contains three (3) items. The third sub-scale was used to measure sessions, it also consists of

Lead City University Ibadan DO NOT COPY

three (3) items. The fourth sub-scale was used to measure user-rule assignment, with three (3) items. Example of these items is "there is an implementation of users' identification and authentication for access to organization's information systems".

3.5 Validity of Research Instrument

To validate this study, the instrument used was acquired from relevant literature analysis and adaptation from questionnaires that have been utilized by other studies. Content validity were established. Content validity was utilized to determine the internal validity of the research instruments, which was verified by the supervisor and other specialists in the information management sector. Comments and all the observations made were incorporated in constructing the final draft of the questionnaire.

3.6 Reliability of the Research Instrument

In guaranteeing the validity of the data, the reliability of the measuring instrument was established through a pilot study. The pilot study helps to ensure consistency and dependability of the scale and the ability to elicit data that answer the research question of the study. The reliability of the instrument was established through administering twenty (20) copies of the questionnaire to twenty Non-Academic Staff of Moshood Abiola Polytechnic, Abeokuta, Ogun State, which is not part of the actual population of the study. The data received Cronbach's alpha values of 0.87 for data handling stages, 0.82 for Access Control, and 0.85 for information security, affirming its reliability and suitability for deployment in the main study.

3.7 Method of Data Collection

Lead City University Ibadan DO NOT COPY

Primary data was collected through a structured questionnaire in accordance with existing research to address the study's objectives. This instrument works well with descriptive survey research because it allows for the collection of data on respondents' opinions and perceptions on current events at a specific point in time. A letter of recommendation was acquired from the Department of Information Management, Lead City University, which was utilized to get authorization to conduct the survey at the State-owned Polytechnics, Oyo State, Nigeria (The Polytechnic, Ibadan, Adeseun Ogundoyin Polytechnic, Eruwa, and Oke-Ogun Polytechnic, Saki). The research instruments were distributed to each respondent, and a brief introduction and clarification were made. Respondents were made aware that the study and data collected are strictly meant for academic research purposes and all responses will remain anonymous.

3.8 Methods of Data Analysis

The data collected were analyzed using descriptive and inferential statistics by the researcher. For research questions one through three, descriptive statistics (mean, frequency distribution, standard deviation, and percentage) were used. The first two null hypotheses were analyzed using inferential statistics, while the third was investigated using multiple regression analysis. All hypotheses in the study were assessed at a significant level of 0.05. Statistical Package and Service Solution (SPSS) Version 22 was used to analyze the data collected for the research.

Lead City University Ibadan DO NOT COPY

Endnotes

1. S.L. Siedlecki, "*Understanding descriptive research designs and methods*." **Clinical Nurse Specialist** 34, (1), (2020): 8-12.

2. Registry Department (Personnel), The Polytechnic, Ibadan, Oyo State Nigeria.

3. Registry Department, Adeseun Ogundoyin Polytechnic, Eruwa, Oyo State Nigeria.

4. Registry Department, The Oke Ogun Polytechnic, Saki, Oyo State Nigeria.

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

6. O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu & C. S. Adigwe. *"Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics."* **Asian Journal of Research in Computer Science.** 17(5), 2024, 140–156. https://doi.org/10.9734/ajrcos/2024/v1 7i5444

7. O. O. Olaniyi. "*Best Practices to Encourage Girls' Education in Maiha Local Government Area of Adamawa State in Nigeria."* **The University of Arkansas Clinton School of Public Service. Research Gate**; 2022. https://doi.org/10.13140/RG.2.2.26144 .25606

8. A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi & S. A. Ajayi. *"Data governance in AI - enabled healthcare systems: A case of the project nightingale."* **Asian Journal of Research in Computer Science.** 17(5), 2024, 85–107. https://doi.org/10.9734/ajrcos/2024/v1 7i5441

Lead City University Ibadan DO NOT COPY

Chapter Four

Results and Discussion of Findings

This chapter outlines the results and corresponding discussions. The first section provides a descriptive analysis through frequency counts, percentages, and means. The second section presents the results related to the research questions and hypotheses that the study aimed to address and test, while the third section discusses the overall findings.

Table 4.1 below provides a descriptive analysis of the response rate through frequency distribution tables. A total of three hundred and ten (285) copies of the questionnaire were administered, and two hundred and seventy-two (272) responses were received. The usable questionnaire represented 95.45% response rate. The following tables 4.1 show the results.

Table 4.1 Analysis of Response Rate

Institutions	Total Administered	Total Received	Percent (%)
The Polytechnic, Ibadan	128	126	46.32
Adeseun Ogundoyin Polytechnic, Eruwa	86	77	28.31
Oke–Ogun Polytechnic, Saki	71	69	25.37
Total	**285**	**272**	**100.0**
Response Rate			**95.45%**

Source: Field Survey, 2025

The demographic analysis of the institutions as presented in Table 4.1 above shows that The Polytechnic, Ibadan has the highest representation with 126 respondents, accounting for 46.32% of the total sample. This is followed by Adeseun Ogundoyin Polytechnic, which recorded 77 respondents, representing 28.31% of the participants. Oke-Ogun Polytechnic, Saki had the least representation with 69 respondents, constituting 25.37% of the total sample. Overall, the total number of respondents across the three institutions was 272, making up 100% of the population surveyed. As shown above, the response rate is 95.45% (272

Lead City ... dan DO NOT COPY

respondents) out of the 100% (285). This distribution indicates that nearly half of the respondents were drawn from The Polytechnic, Ibadan, while the remaining proportion was fairly shared between Oke-Ogun Polytechnic, Saki, and Adeseun Ogundoyin Polytechnic, Eruwa.

4.1 Demographic Data Analysis

This section provides an overview of the demographic characteristics of the individuals who participated in the study.

Table 4.2 Demographic Information of Non-Academic Staff in Oyo State-Owned Polytechnics (n=272)

Variables	Category	Frequency	Percentage
Gender	Male	132	48.5%
	Female	140	51.5%
Age	20 – 25years	24	7.0%
	26 - 30years	16	6.8%
	31 - 35years	48	16.6%
	36 - 40years	24	7.0%
	41 – 45years	32	10.8%
	46years above	128	51.9%
Educational Qualification	NCE/OND	44	16.2%
	HND	124	45.6%
	B.Sc	60	22.1%
	M.Sc.	44	16.2%
	P.hD	0	0%

Lead City University Ibadan DO NOT COPY

Work Experience	5 - 10years	4	1.5%
	11 - 15years	40	14.7%
	16 -20years	48	17.6%
	21 – 25years	16	5.9%
	26 – 30years	164	60.3%

Source: Field Survey Data (2025)

The demographic information of Non-Academic Staff in Oyo State-owned polytechnics, as shown in Table 4.2 above, it indicates a slight dominance of female staff (140, 51.5%) over their male counterparts (132, 48.5%).

In terms of 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

Lead City University Ibadan DO NOT COPY

staff (14.7%) had served for 11–15 years. A smaller proportion of 16 respondents (5.9%) had 21–25 years of experience, and majority of respondents 164 (60.3%) had worked for 26–30 years, showing that long-serving staff are relatively more and have good experience.

Summarily, the demographic data of Non-Academic Staff in Oyo State-owned polytechnics reveals a slight predominance of female employees and a notable presence of older staff members. Most individuals possess mid-level educational qualifications, and a minority have relatively short work experience. This suggests that, while there are experienced personnel, many staff members are still getting familiarised with their roles. It was observed that the majority of the respondents, ranging from age 20 to 35, who formed 30% of the respondents, are either casual or part-time staff, which prompts the necessity for the state government to recruit more staff, as people in this age range may not handle the institution's information properly since they believe they have nothing at stake. Also, the majority of these respondents are HND holders, which indicates that most of them are in the Executive cadre (Chief Executive Officers, Principal Executive Officers, Senior Executive Officers, Executive Officers and Clerical Officers). Therefore, the findings highlighted the importance of providing ongoing training and retraining programs, with proper mentorship to support the professional growth of Non-Academic Staff, as well as strategies aimed at retaining and employing experienced employees.

Lead City University Ibadan DO NOT COPY

4.2 Presentation of Data

This section presents analysis of research questions and hypotheses testing in related to this research work.

4.2.1 Analysis of Research Questions

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

Table 4.3 Descriptive Statistics for Information Security

Information Security	VH	H	L	VL	Mean
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**

Lead City University Ibadan DO NOT COPY

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
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**

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

Source: Field survey, 2025

The examination of Table 4.3 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%)

Lead City University Ibadan DO NOT COPY

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 unauthorised 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.

Summarily, the weighted mean for all elements of information security was 3.10, signifying that employee perceptions of the organization's information security practices are highly

Lead City University Ibadan DO NOT COPY

elevated. Key competencies encompass backup protocols, documentation safeguarding, and information storage administration. Nonetheless, deficiencies in operational standards, prohibitions on unauthorized software, and the handling of physical media in transit underscore potential enhancements to fortify the security architecture. A majority of respondents expressed confidence in protocols for new information systems, but fewer rated network operating guidelines highly. Strong support was evident for the safeguarding of system documentation, particularly concerning confidentiality. In terms of information integrity, many employees acknowledged the importance of separating development, testing, and operational facilities, with the backup policy receiving particularly favorable ratings. Conversely, evaluations of electronic messaging security and system usage oversight were less positive. Regarding information availability, substantial support was noted for information management and storage, although the physical transport of media received mixed reviews.

Research Question Two: What is the level of data handling stages by Non-Academic Staff in Oyo State-owned Polytechnics?

Table 4.4 Descriptive Statistics on Data Handling Stages

Data Handling Stages	**SA**	**A**	**D**	**SD**	**Mean**
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**	**Mean**
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

Lead City University Ibadan DO NOT COPY

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

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: SA=Strongly Agree, A=Agree, D=Disagree, SD=Strongly Disagree

Source: Field survey, 2025

The analysis shown in Table 4.4 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%)

Lead City University Ibadan DO NOT COPY

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

Lead City University Ibadan DO NOT COPY

(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.

Summarily, the results show that Non-Academic Staff demonstrate a moderate to near-high level of practice in data handling policies. Strong performance was observed in metadata creation, data planning, and information verification (means ranging from 2.94 to 2.99, with low variability), whereas weaker performance was noted in assigning permanent identifiers to datasets (mean = 2.81, SD = 0.463). This suggests that while data handling practices are fairly consistent across polytechnics, there is still a need to strengthen data classification and archiving mechanisms and to establish more rigorous policy frameworks to ensure consistent compliance with best practices.

Research Question Three: What is the level of access control by the registry of staff of Oyo State-owned Polytechnics?

Table 4.5 Descriptive Statistics on Access Control

Access Control	**VH**	**H**	**L**	**VL**	**Mean**
Roles Definition					
Mode of equipment identification	(80) 29.4%	(152) 55.9%	(40) 14.7%	(0) 0.00%	3.15
Separation of data networks into domains according to their function	(48) 17.6%	(160) 58.8%	(64) 23.5%	(0) 0.00%	2.94
Routing implementation to enforce access control policy	(44) 16.2%	(176) 64.7%	(52) 19.1%	(0) 0.00%	2.97
Average Mean for Roles					**3.02**
Permissions Allocation Control	**VH**	**H**	**L**	**VL**	**Mean**

Lead City University Ibadan DO NOT COPY

User password guideline control	(92) 33.8%	(148) 54.4%	(32) 11.8%	(0) 0.00%	3.22
Periodic review of user access rights	(48) 17.6%	(176) 64.7%	(48) 17.6%	(0) 0.00%	3.00
User guideline for the usage of passwords	(84) 30.9%	(152) 55.9%	(36) 13.2%	(0) 0.00%	3.18
Average Mean for Permissions					**3.13**
Sessions Management	**VH**	**H**	**L**	**VL**	**Mean**
Clear desk and screen policy	(68) 25.0%	(156) 57.4%	(48) 17.6%	(0) 0.00%	3.07
Existence of policies for the use of data network services	(64) 23.5%	(152) 55.9%	(56) 20.6%	(0) 0.00%	3.03
Authentication of remote users	(76) 27.9%	(136) 50.0%	(6) 22.1%	(0) 0.0%	3.06
Average Mean for Sessions					**3.05**
User Assignments Control	**VH**	**H**	**L**	**VL**	**Mean**
Restriction on users' ability to connect to data network	(80) 29.4%	(144) 52.9%	(48) 17.6%	(0) 0.0%	3.12
Incorporating users authentication for access to institution information system	(56) 20.6%	(184) 67.6%	(32) 11.8%	(0) 0.00%	3.09
Understanding time frame for connecting to information system	(76) 27.9%	(148) 54.4%	(48) 17.6%	(0) 0.0%	3.10
Average Mean for Relationship Management					**3.10**
Weighted Mean for Access Control					**3.15**

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: SA=Strongly Agree, A=Agree, D=Disagree, SD=Strongly Disagree

Source: Field survey, 2025

The results in Table 4.5 reveal that the overall weighted mean score for access control was 3.15, which falls within the high category (decision rule: 3.00–4.00 = High). This indicates

Lead City University Ibadan DO NOT COPY

that Non-Academic Staff in Oyo State-owned Polytechnics generally demonstrate strong compliance with access control measures.

For the roles definition dimension, the average mean was 3.02, suggesting a high level of implementation. Specifically, 80 respondents (29.4%) rated the presence of automatic equipment identification as very high and 152 (55.9%) as high, while only 40 (14.7%) rated it low, producing a mean of 3.15 and standard deviation of 0.649. Similarly, 48 staff (17.6%) rated network separation into domains as very high, 160 (58.8%) rated it high, and 64 (23.5%) rated it low, yielding a mean of 2.94. For routing implementation, 44 (16.2%) rated it very high, 176 (64.7%) high, and 52 (19.1%) low, resulting in a mean of 2.97. These results indicate that while access control roles are generally well implemented, network separation appears slightly weaker than other aspects.

In the area of permissions, the average mean was 3.13, reflecting stronger compliance. A user password guideline was rated very high by 92 respondents (33.8%) and high by 148 (54.4%), with only 32 (11.8%) rating it low, giving a mean of 3.22 and standard deviation of 0.639. Similarly, periodic review of user access rights was rated very high by 48 (17.6%) and high by 176 (64.7%), though 48 (17.6%) rated it low, resulting in a mean of 3.00. A user guideline for password selection and usage was endorsed by 84 (30.9%) at very high and 152 (55.9%) at high, while 36 (13.2%) rated it low, giving a mean of 3.18. This shows that password guidelines and management are well established, though periodic review practices are less consistent.

The sessions dimension recorded an average of 3.05, also in the high category. For emotional control during high-pressure situations, 68 respondents (25.0%) rated very high, 156 (57.4%) high, and 48 (17.6%) low, producing a mean of 3.07. Staying calm during conflicts was rated very high by 64 (23.5%) and high by 152 (55.9%), while 56 (20.6%) rated low, with a mean

Lead City University Ibadan DO NOT COPY

of 3.03. Optimism during difficulties was rated very high by 76 (27.9%) and high by 136 (50.0%), while 60 (22.1%) rated low, producing a mean of 3.06. These results suggest that staff exhibit a generally high level of emotional stability in session management, though about one-fifth still report lower performance.

Finally, the user–role assignment dimension had an average mean of 3.10, confirming strong compliance. Restrictions on users' ability to connect to the network were rated very high by 80 respondents (29.4%) and high by 144 (52.9%), while 48 (17.6%) rated low, producing a mean of 3.12. User identification and authentication were rated very high by 56 (20.6%) and high by 184 (67.6%), though 32 (11.8%) rated low, giving a mean of 3.09. Guidelines for connection time to systems were endorsed very highly by 76 (27.9%) and highly by 148 (54.4%), while 48 (17.6%) rated low, resulting in a mean of 3.10. This shows strong institutional practice in ensuring proper user restrictions and authentication measures.

In summary, the findings indicate that Non-Academic Staff maintain a high level of access control overall (weighted mean= 3.15), with particularly strong practices in user password guidelines (mean= 3.22) and network access restrictions (mean= 3.12). However, weaker areas include network separation into domains (mean = 2.94) and periodic review of user access rights (mean= 3.00).

Lead City University Ibadan DO NOT COPY

4.2.2 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 4.6a: 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 4.6b:

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 4.6c:

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 4.5a, 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.

Table 4.5b 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

Lead City University
T COPY

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 4.5c reveal varied contributions. Data classification (β = .206, t = 3.251, p = .001) and data scheduling and maintenance (β = .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 (β = –.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 (β = –.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.

H_02: There is no significant influence of access control on information security among Non-Academic Staff of Oyo State-owned Polytechnics.

Table 4.7a: Influence of Access Control (Roles Definition, Permissions Allocation Control, Session Management, and User Assignment Control) on

Lead City University Ibadan DO NOT COPY

Information Security Among Non-Academic Staff of Oyo State-Owned Polytechnics

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.707[a]	.499	.492	.28894

a. Predictors: (Constant), User Assignment Control, Permissions Allocation, Roles Definition, Sessions Management

Table 4.7b:

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	22.240	4	5.560	66.598	.000[b]
	Residual	22.290	267	.083		
	Total	44.530	271			

a. Dependent Variable: Information Security Practice

b. Predictors: (Constant), User Assignments Control, Permissions Allocation, Roles Definition, Sessions Management

Table 4.7c:

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.134	.124		9.137	.000
	Roles Definition	.309	.045	.393	6.889	.000
	Permissions Allocation Control	.160	.048	.208	3.309	.001
	Sessions Management	.093	.052	.126	1.799	.073
	User Assignments Control	.083	.052	.107	1.592	.113

a. Dependent Variable: Information Security Practice

As presented in Table 4.6a, the model yielded a correlation coefficient of R = .707, indicating a strong positive relationship between access control measures and information security. The coefficient of determination (R^2 = .499) shows that approximately 49.9% of the variance in information security practices can be explained by access control dimensions. The adjusted R^2 of .492 confirms that after controlling for model complexity, the predictors still account for nearly half of the variation in security practices, which is a very substantial contribution.

The analysis of variance in Table 4.6b demonstrates that the overall model was statistically significant ($F(4,267) = 66.598$, $p < .001$). This indicates that the combined influence of roles

definition, permissions allocation, sessions management, and user assignments control on information security is significant. Therefore, the null hypothesis (H02) is rejected, confirming that access control significantly influences information security among Non-Academic Staff in Oyo State-owned Polytechnics.

The regression coefficients in Table 4.6c provide insight into the relative contributions of each predictor. Roles (β = .393, t = 6.889, p < .001) emerged as the strongest positive predictor, suggesting that proper role assignment and network-level controls are critical in promoting secure practices. Permissions (β = .208, t = 3.309, p = .001) also had a significant positive effect, indicating that password guidelines and access right reviews substantially strengthen security. However, sessions (β = .126, t = 1.799, p = .073) and user assignments control (β = .107, t = 1.592, p = .113) were not statistically significant predictors at the 0.05 level, though they contributed positively in the model.

Access control policies significantly influence information security, explaining nearly half of the observed variance in practices. Among the dimensions, roles definition and permissions allocation are the most important drivers, while sessions and user assignments control have positive but non-significant effects. This suggests that strengthening role-based access and permission management mechanisms would yield the greatest improvements in institutional information security.

$H_0$3: There is no combined influence of emotional intelligence and leadership effectiveness on the employees' wellbeing of Secretarial Staff in the Government Secretariat, Oyo State, Nigeria

Table 4.8a: Influence of Data Handling Stages and Access Control on Information Security Among Non-Academic Staff of Oyo State-Owned Polytechnics.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.700[a]	.490	.486	.29051

Lead City University Ibadan DO NOT COPY

a. Predictors: (Constant), Access Control, Data Handling Stages

Table 4.8b:

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	21.827	2	10.914	129.311	.000[b]
	Residual	22.703	269	.084		
	Total	44.530	271			

a. Dependent Variable: Information Security Practice
b. Predictors: (Constant), Access Control, Data Handling Stages

Table 4.8c:

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.156	.393		.398	.691
	Data Handling Stages	.387	.141	.125	2.752	.006
	Access Control	.595	.041	.655	14.438	.000

a. Dependent Variable: Information Security Practice

As shown in Table 4.7b, the regression model was statistically significant ($F(2,269) = 129.311$, $p < .001$). This indicates that data handling stages and access control jointly exert a significant influence on information security. The model explained a substantial proportion of variance in information security practices, with the regression sum of squares (21.827) accounting for nearly half of the total variation (44.530).

The regression coefficients in Table 4.7c further reveal the relative contributions of the predictors. Access control was the strongest predictor ($\beta = .655$, $t = 14.438$, $p < .001$), suggesting that robust access control practices, such as role management, permissions, and authentication measures play a critical role in enhancing security. Data handling stages also had a significant positive effect ($\beta = .125$, $t = 2.752$, $p = .006$), indicating that improvements in data creation, classification, scheduling, and usage contribute meaningfully, though less strongly, to information security outcomes.

Lead City University Ibadan Digital Library

The constant term (.156, p = .691) was not statistically significant, which implies that without the influence of access control and data handling stages, information security practices cannot be adequately explained.

The findings confirm that data handling stages and access control jointly have a significant influence on information security among Non-Academic Staff in Oyo State-owned Polytechnics. However, access control emerged as the dominant predictor, exerting a stronger influence than data handling stages. Therefore, the null hypothesis (H_{03}) is rejected.

4.3 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.

Lead City University Ibadan DO NOT COPY

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 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[5,6,7,8].

Access control mechanisms scored particularly well, with a high compliance average of 3.15. This indicates that staff are generally following access control measures effectively. The regression analysis reinforces this, showing that access control significantly impacts information security practices, accounting for nearly 49.9% of the variance observed. This underscores the necessity of aligning access rights with specific job responsibilities, which helps protect both institutional assets and the privacy of students and staff. The findings of this study support some discussions by scholars on data governance in AI-enabled healthcare systems, fine-grained access control in the era of cloud computing, and systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment[9,10,11].

The findings from the hypothesis testing provide a comprehensive understanding of how data handling stages and access control mechanisms influence information security practices among Non-Academic Staff in Oyo State-owned Polytechnics. This section delves deeper

Lead City University Ibadan DO NOT COPY

into the implications of these findings, exploring the interrelationships between the variables and their significance in enhancing information security.

The results indicate a moderate positive correlation (R = 0.421) between data handling stages and information security practices, with an R^2 value of 0.177. This suggests that approximately 17.7% of the variance in information security can be attributed to the effectiveness of data handling procedures. While this may seem modest, it highlights the critical role that systematic data management plays in fortifying security measures.

Among the data handling stages, data classification (β = 0.206) and data scheduling and maintenance (β = 0.353) emerged as particularly influential predictors of information security. These findings underscore the necessity for educational institutions to implement robust classification systems that categorize data based on sensitivity and usage. Effective classification not only facilitates compliance with legal frameworks but also enhances operational efficiency by ensuring that sensitive information is readily identifiable and appropriately protected.

Moreover, the strong positive influence of data scheduling and maintenance indicates that systematic approaches to managing data, such as regular updates, backups, and archiving, are vital for maintaining data integrity and accessibility. Institutions that prioritize these practices are likely to experience fewer incidents of data breaches, thereby reinforcing trust among stakeholders.

Conversely, the data creation dimension yielded a non-significant predictor (β = -0.016, p = 0.785), suggesting that current practices related to metadata documentation and file planning may not directly enhance security outcomes. This gap indicates a potential area for

Lead City University Ibadan DO NOT COPY

improvement, as institutions typically rely on accurate data creation processes to ensure the reliability of information.

The negative influence of the use of information (β = -0.130, p = 0.043) further suggests that while data is utilized for decision-making and operational processes, inconsistencies or potential misuse could undermine security efforts. This finding highlights the need for continuous training and clear guidelines on data usage among Non-Academic Staff. It suggests that educational efforts should focus not only on technical competencies but also on instilling a culture of responsibility and awareness regarding the implications of data handling practices.

The analysis of access control mechanisms revealed a robust positive correlation (R = 0.707) with information security practices, with an R^2 value of 0.499. This finding indicates that nearly 50% of the variance in information security can be explained by the effectiveness of access control measures. This underscores the crucial role that well-structured access control systems play in mitigating risks associated with unauthorized access, particularly in environments handling sensitive information.

Among the access control dimensions, roles definition emerged as the strongest predictor (β = 0.393), highlighting the importance of aligning access rights to specific job functions. This alignment minimizes the risk of insider threats by ensuring that Non-Academic Staff have access only to the information necessary for their roles. Such a structured approach not only enhances security but also promotes operational efficiency by streamlining the process of granting and revoking access as staff roles evolve.

The significant positive effect of permissions allocation (β = 0.208) reinforces the necessity for institutions to establish clear guidelines for managing access rights. This includes

Lead City University Ibadan DO NOT COPY

implementing strict password policies, regular reviews of permissions, and ensuring that staff are aware of their responsibilities regarding data security. The findings suggest that institutions should invest in training programs that not only educate staff on the technical aspects of access control but also emphasize the broader implications of their access rights in the context of information security.

While session management and user assignments control were found to have positive contributions, they were not statistically significant predictors at the 0.05 level. This suggests that while these elements are important for maintaining a secure environment, their effectiveness may be enhanced through better implementation and regular review processes. Institutions should focus on refining their policies surrounding session management to ensure that they are not only practical but also adaptable to changing operational needs.

The study further reveals that data handling stages and access control jointly exert a significant influence on information security practices. The regression analysis indicated that these independent variables together explain a substantial proportion of the variance in information security practices, reinforcing the interconnectedness of these elements in shaping effective security strategies. The findings affirm that addressing both data handling and access control is essential for establishing a comprehensive information security framework. Institutions that recognize the interplay between these areas are better positioned to safeguard sensitive information and respond effectively to emerging threats.

The implications of these findings extend beyond academic discourse, offering critical insights for institutional policy and practice. Given the evolving landscape of cyber threats, it is imperative for Oyo State-owned Polytechnics to develop and implement comprehensive data handling policies that are consistently enforced. This includes establishing clear

Lead City University Ibadan DO NOT COPY

guidelines for data classification, scheduling, and maintenance, as well as refining access control measures to align with the specific needs of Non-Academic Staff. Furthermore, continuous training and professional development are essential for fostering a culture of security awareness among staff. While equipping Non-Academic Staff with the necessary knowledge and skills, institutions can enhance their overall security posture and mitigate the risks of insider threats.

Lead City University Ibadan DO NOT COPY

Endnotes

1. O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu & C. S. Adigwe. "*Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics*." **Asian Journal of Research in Computer Science.** 17(5), 2024, 140–156. https://doi.org/10.9734/ajrcos/2024/v1 7i5444

2. N. D., Nte, V. A., Teru, & A., Ridwan, "*Challenges of Information Security Laws and Legislations in Nigeria's Institutions of Higher Education: Views from Yola, Adamawa State*." **Research and Development in Education**, 4(8,12), 2024, 1498–1519. https://doi.org/10.22219/raden.v4i2.35711

3. B. C. E, Oguguo, & A. O., Christopher. "*Cybersecurity: A Tool for Curbing Examination Breaches and Improvement of the Quality of Large-Scale Educational Assessments*." **Information Security Journal**: A Global Perspective 33(4), 2024, 12-13 https://doi.org/10.1080/19393555.2023.2284761

4. S., Prabhu & T., Nik. "*A Primer on Insider Threats in Cybersecurity*." **Information Security Journal**: A Global Perspective 31(5), 2022, 608-609. https://doi.org/10.1080/19393555.202 1.1971802

5. O. O. Olaniyi. "*Best Practices to Encourage Girls' Education in Maiha Local Government Area of Adamawa State in Nigeria.*" **The University of Arkansas Clinton School of Public Service. Research Gate**; 2022. https://doi.org/10.13140/RG.2.2.26144 .25606

6. S. S., Bakare, O. A. Adekunle, et al. "*Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations*." **Computer Science & IT Research Journal,** Volume 5, Issue 3529-539 (2024).

7. A., Djenna, U., Bodin, & O., Schelen, "*Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts*." **IEEE Access**, 11, 2023, 10193–10195. https://doi.org/10.1109/access.2023.3240000

8. D. A., Adebanjo, G., Chigbu, & C. M. Osazuwa. "*Effect of Data Protection Frameworks against Cybercrimes on Cyber Security in Nigeria*." **The American Journal of Political Science Law and Criminology** 6(09), 2024, 64-84.

9. A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi & S. A. Ajayi. "*Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale*." **Asian Journal of Research in Computer Science**. 17(5), 2024, 85–107. https://doi.org/10.9734/ajrcos/2024/v1 7i5441

10. K. Albulayhi, A. Abuhussein, et al. "*Fine-Grained Access Control in the era of Cloud Computing: An Analytical Review*." **10th Annual Computing and Communication Workshop and Conference (CCWC)**, 2020, 0748-0755. IEEE.

11. M. Ayedh, T. Aljuaid, A. W. Abdul Wahab, and M. Y. Idna Idris. "*Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions*." **Applied Sciences** 13(14), 2023, 8048. https://doi.org/10.3390/app13148048

Lead City University Ibadan DO NOT COPY

Chapter Five

Summary, Conclusion and Recommendations

This chapter presents, discusses, and summarizes the key findings of the study, drawing conclusions and offering practical recommendations. It also outlines the study's contribution to knowledge and suggests areas for further study.

5.1 Summary of Findings

This study investigated "Data Handling Stages, Access Control and Information Security Practice among Non-Academic Staff in State-owned Polytechnics, Oyo State, Nigeria". Based on the objectives of the study which are; to assess the level of information security practice by non-academic staff in State-owned Polytechnics, Oyo State, Nigeria; examine the data handling stages that exist in State-owned Polytechnics, Oyo State, Nigeria; to identify the level of access control by non-academic staff in State-owned Polytechnics, Oyo State, Nigeria; to determine the influence of data handling stages on information security practice among non-academic staff in State-owned Polytechnics, Oyo State, Nigeria; to ascertain the influence of access control on information security practice among non-academic staff of State-owned Polytechnics, Oyo State, Nigeria; and to determine the combined influence of data handling stages and access control on information security practice among non-academic staff in Oyo State-owned Polytechnics, Oyo State, Nigeria, research questions were raised, hypotheses were formulated, data were collected and analyzed descriptively and inferentially.

The study found a high level of information security practice by non-academic staff in these institutions; a high level of data handling stages by non-academic staff in these institutions; a high level of access control by the non-academic staff these institutions; that data handling stages significantly and positively influences information security practice among non-academic staff in these institutions; that access control significantly and positively influence

Lead City University Ibadan DO NOT COPY

information security practice among non-academic staff in these institutions; and that data handling stages and access control significantly influence information security practice among non-academic staff of these institutions.

5.2 Conclusion

This study has yielded significant insights into the relationship between data handling stages, access control, 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. Notably, the study also indicated that Non-Academic Staff show strong practices in critical areas like safeguarding of system documentation and adherence to backup protocols. These elements are vital for maintaining data integrity and ensuring the availability of information to the right users when needed. 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

Lead City University Ibadan DO NOT COPY

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

Access control mechanisms were evaluated positively, which indicates a strong compliance level among Non-Academic Staff in adhering to access control measures. The regression analysis further confirmed that access control significantly influences information security practices, explaining approximately 49.9% of the variance observed. Among the access control dimensions, roles definition and permissions allocation emerged as the most significant predictors, reinforcing the necessity of aligning access rights with job responsibilities. This alignment is crucial for minimizing the risk of data breaches, thus safeguarding both institutional assets and the privacy of students and staff. Moreover, the study illuminated several challenges that institutions face, including inadequate funding for security infrastructure, the need for regular reviews and updates of user access rights, and the overall necessity for a culture of security awareness among staff. These challenges are compounded by the evolving landscape of cyber threats, which necessitate continuous adaptation and vigilance. The role of training and awareness programs for staff emerged as a critical factor in reinforcing effective security measures. Conclusively, this research highlights the interconnectedness of data handling policies, access control, and information security practices within Oyo State-owned Polytechnics, Nigeria.

Lead City University Ibadan DO NOT COPY

5.3 Recommendations

Based on the findings of this study, several recommendations are proposed to enhance data handling policies, access control measures, and overall information security practices among Non-Academic Staff in Oyo State-owned Polytechnics. These recommendations aim not only

to address the identified gaps but also to foster a culture of security awareness and proactive engagement within the institutions. These recommendations are as follows:

1. Institutional management should prioritize regular training programs for Non-Academic Staff, focusing on key areas such as information security, data handling procedures, and access control protocols. These trainings not only build technical competence but also foster a culture of accountability and awareness.
2. Institutions must develop clear and enforceable data handling policies that outline procedures for data classification, storage, and archiving. These policies should define categories of data based on sensitivity and usage, ensuring that confidential information is appropriately protected and easily retrievable when needed. A well-structured policy framework enhances operational efficiency, supports legal compliance, and provides staff with consistent guidelines for managing institutional data responsibly.
3. To remain effective, data handling policies should be subject to periodic review and revision. As technology evolves and new threats emerge, institutions must ensure that their policies reflect current best practices and regulatory standards. Regular updates also allow for the integration of feedback from staff and stakeholders, ensuring that the policies remain practical, relevant, and aligned with institutional goals.
4. Effective data governance also requires continuous oversight of how information is accessed, shared, and utilized within the institution. Management should implement monitoring systems that track data usage patterns and flag irregularities. This includes ensuring that data is used ethically and in accordance with institutional policies. Proper implementation safeguards against misuse, supports transparency, and reinforces trust among staff and stakeholders.

Lead City University Ibadan DO NOT COPY

5. Institutions must establish mechanisms to monitor system activity and detect the presence of unauthorized software. Unregulated applications pose significant security risks, including malware infections and data leaks. Through conducting regular audits, enforcing software approval protocols, and educating staff on the dangers of unauthorized installations, management can maintain a secure digital environment and uphold institutional integrity.
6. Access control should be dynamic and responsive to changes in job roles and responsibilities. Management should implement a structured schedule for reviewing user access rights, ensuring that permissions remain appropriate and limited to what is necessary for each role. This minimizes the risk of unauthorized access and insider threats, while also streamlining operational workflows. Clear documentation and automated review systems can further enhance the effectiveness of this process.

5.4 Contributions to Knowledge

This study on "Data Handling Stages, Access Control, and Information Security Practice among Non-Academic Staff in State-Owned Polytechnics, Oyo State, Nigeria" makes several significant contributions to the existing body of knowledge. First, it provides a contextual understanding of data handling practices and information security challenges specific to Nigerian academic institutions. This research addresses a gap in the literature, which predominantly emphasizes developed countries, thus shedding light on the unique circumstances faced by institutions in a developing context like Nigeria. Furthermore, the study highlights the interconnectedness of data handling policies, access control, and information security practices, illustrating how these elements work collaboratively to enhance overall information security practices. This integrated perspective not only enriches

Lead City University Ibadan DO NOT COPY

the theoretical frameworks surrounding information management but also offers practical insights that can inform future research and institutional practices.

Through vigorous empirical methodology, including quantitative analysis of data collected from Non-Academic Staff in Oyo State-owned Polytechnics, the findings present concrete evidence regarding the current state of information security practices. This empirical basis strengthens the theoretical discourse and provides a foundation for further inquiry. The research also offers actionable recommendations for improving data handling policies and access control mechanisms, through the management of these institutions in their efforts to enhance information security practices. The emphasis on training and awareness among Non-Academic Staff underscores the importance of the human factor in effective information security.

Lastly, the examination of compliance with legal frameworks, such as the GDPR, provides valuable insights for institutions striving to meet regulatory requirements while safeguarding sensitive information. In sum, this study not only enriches the academic discourse on information security in Oyo State-owned polytechnics but also serves as a practical resource for administrators and policymakers seeking to improve data management and security practices in educational contexts.

5.5 Suggested Area of Further Studies

In light of the findings and contributions of this study, several avenues for further research emerge, each presenting an opportunity to deepen our understanding of information security practices in academic settings, future researchers are encouraged to;

1. Explore the same topic using alternative theoretical frameworks beyond those employed in this study.

Lead City University Ibadan DO NOT COPY

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.

Lead City University Ibadan DO NOT COPY

Bibliography

Books

Afshar, A. Authentication, Authorization, and Selective Disclosure for IoT Data Sharing Using Verifiable Credentials and Zero-Knowledge Proofs. **Lecture Notes in Computer Science**, 2023, 88–101.

Griffin A. & Mazikana P. (2007) "Fostering Trust and Transparency in Governance: Investigating and Addressing the Requirements for Building Integrity in Public Sector Information Systems in the ICT Environment". **IRMT, London**, 2007.

Whitman, Michael E., and Herbert J. Mattord. "Principles of information security". **Boston, MA: Thomson Course Technology**, 2009. http://ndl.ethernet.edu.et/bitstream/123456789/89363/1/Principles%20of%20Information%20Security%20by%20Whitman%2C%20Michael%20Mattord%2C%20Herbert%20.pdf

Peer-Reviewed Journal Articles

Aathilakshmi, S., A. Prasanth, KK Devi Sowndarya, and Pham Chien Thang. "Access Control Using AI Based Biometric Systems: Case Study." In **AI Based Advancements in Biometrics and its Applications**, 156-171. CRC Press, 2024.https://doi.org/10.1201/9781032702377-9

Aboukadri, Sara, Aafaf Ouaddah, and Abdellatif Mezrioui. "Machine learning in identity and access management systems: Survey and deep dive." **Computers & Security** 139 (2024): 103729. https://doi.org/10.1016/j.cose.2024.103729

Adebiyi, O.O., Olabanji, S.O. , & Olaniyi, O.O. "Promoting inclusive accounting education through the integration of stem principles for a diverse classroom." **Asian Journal of Education and Social Studies,** 49(4), 2023:152–171. DOI:https://doi.org/10.9734/ajess/2023/v49 i41196

Adenekan, Tolulope Elizabeth, and Oluwatosin Abiodun Ologbosere. "Information Security Policy and Practices among Office Managers in Telecommunications Industry in Nigeria." **International Journal of Advanced Research in Multidisciplinary Studies (IJARMS)**, 1 (1), 2021: 70-78

Adigwe, Chinasa Susan, Oluwaseun Oladeji Olaniyi, Samuel Oladiipo Olabanji, Olalekan J. Okunleye, Nanyeneke Ravana Mayeke, and Samson Abidemi Ajayi. "Forecasting the future: The interplay of artificial intelligence, innovation, and competitiveness and its effect on the global economy." **Innovation, and Competitiveness and its Effect on the Global Economy** (2024). DOI:https://doi.org/10.9734/ajeba/2024/v24 i41269 Njoku

Lead City University, Ibadan DO NOT COPY

Afshar, A. Authentication, Authorization, and Selective Disclosure for IoT Data Sharing Using Verifiable Credentials and Zero-Knowledge Proofs. Lecture Notes in Computer Science, 2023: 88–101. https://doi.org/10.1007/978-3-031-25467-3_6

Ahmadi, Sina. "Zero trust architecture in cloud networks: Application, challenges and future opportunities." **Journal of Engineering Research and Reports** 26 (2), 2024: 215-228. https://doi.org/10.9734/jerr/2024/v26i2.1083

Ajayi, Samson Abidemi, Oluwaseun Oladeji Olaniyi, Tunboson Oyewale Oladoyinbo, Nneka Damola Ajayi, and Folashade Gloria Olaniyi. "Sustainable sourcing of organic skincare ingredients: A critical analysis of ethical concerns and environmental implications." **Asian Journal of Advanced Research and Reports** 18 (1), 2024: 65-91. DOI: https://doi.org/10.9734/ajarr/2024/v18i 1598

Aladesanmi, O., Afolabi, B., & Oyebisi, T. O. Assessing Network Services and Security in Nigeria Universities. Journal of Computer Science and Information Technology, 19 (1), (2012): 60–66. https://doi.org/10.4314/JCSIA.V19I1.8

Albulayhi, Khalid, Abdullah Abuhussein, Faisal Alsubaei, and Frederick T. Sheldon. "Fine-grained access control in the era of cloud computing: An analytical review." **10th Annual Computing and Communication Workshop and Conference (CCWC)**, 2020: 0748-0755. IEEE DOI:https://doi.org/10.1109/ccwc47524.20 20.9031179

Al-Mhiqani, Mohammed Nasser, Rabiah Ahmad, Z. Zainal Abidin, Warusia Yassin, Aslinda Hassan, Karrar Hameed Abdulkareem, Nabeel Salih Ali, and Zahri Yunos. "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations." **Journals of Applied Sciences** 10 (15), 2020: 5208. DOI: https://doi.org/10.3390/app10155208

Alraja, Mansour Naser, Usman Javed Butt, and Maysam Abbod. "Information security policies compliance in a global setting: An employee's perspective." **Journal of Computers & Security** 129, 2023: 103208. https://doi.org/10.1016/j.cose.2023.103208

Alshammari, Salah T., Aiiad Albeshri, and Khalid Alsubhi. "Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services." **Symmetry** 13 (3), 2021:492. DOI: https://doi.org/10.3390/sym13030492

Alsowail, R. A., & Al-Shehari, T. A multi-tiered framework for insider threat prevention. Electronics, 10(9), 2021: 1005. https://doi.org/10.3390/electronics10091005

Alsowail, Rakan A., and Taher Al-Shehari. "A multi-tiered framework for insider threat prevention." **Electronics** 10 (9), 2021: 1005. https://doi.org/10.3390/electronics100 91005

Alsowail, Rakan A., and Taher Al-Shehari. "Empirical detection techniques of insider threat incidents." **IEEE Access** 8, 2020: 78385-78402.

Lead City University Ibadan DO NOT COPY

Ameer, Safwa, Benson, James, & Sandhu, Ravi. “An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach.” **Journal of Information**, 13(2), 2022: 60. Department of Computer Science, Institute for Cyber Security and CREST C-SPECC, The University of Texas at San Antonio, San Antonio, TX 78249, USA https://doi.org/10.3390/info13020060

Arigbabu, Aisha Temitope, Oluwaseun Oladeji Olaniyi, Chinasa Susan Adigwe, Olubukola Omolara Adebiyi, and Samson Abidemi Ajayi. "Data governance in AI-enabled healthcare systems: A case of the project nightingale." **Asian Journal of Research in Computer Science** 17 (5), 2024: 85-107. DOI:https://doi.org/10.9734/ajrcos/2024/v17i5441

Awad A. I., Babu A., Barka E. & Shuaib K. “AI-powered biometrics for Internet of Things security: A review and future vision”. **Journal of Information Security and Applications**, 2024. https://doi.org/10.1016/j.jisa.2024.103748

Ayedh M, Aljuaid Turkea, Ainuddin Wahid Abdul Wahab, and Mohd Yamani Idna Idris. "Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions." **Applied Sciences,** 13 (14), 2023: 8048. https://doi.org/10.3390/app13148048

Azad, Muhammad Ajmal, Junaid Arshad, Shazia Mahmoud, Khaled Salah, and Muhammad Imran. "A privacy-preserving framework for smart context-aware healthcare applications." **Transactions on Emerging Telecommunications Technologies** 33 (8), 2022: e3634. DOI: https://doi.org/10.1002/ett.3634

Badamasi, Bukhari, and Samuel C. Avemaria Utulu. "Framework for managing cybercrime risks in Nigerian universities." arXiv preprint arXiv:2108.09754 **Computers and Society** (2021). https://dblp.uni-trier.de/db/journals/corr/corr2108.html#abs-2108-09754

Bakare, Seun Solomon, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh. "Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations." (2024).

Barata, Kimberly, Ray Bennett, Piers Cain, and Dawn Routledge. "From accounting to accountability: managing financial records as a strategic resource." Tanzania: a case study. **International Records Management Trust/Rights and Records Institute** http://www.irmt.org/download/DOCUME% 7E1/DEVELO% 7E1/RESEAR% 7E1/TANZAN% 7E1. PDF (Accessed 17 October 2007) (2001).

Baumer, Thomas, Mathis Müller, and Günther Pernul. "System for cross-domain identity management (SCIM): Survey and enhancement with RBAC." **IEEE Access,** 11 (2023): 86872-86894. https://doi.org/10.1109/access.2023.3304270

Boopathi, S. "Securing Healthcare Systems Integrated With IoT: Fundamentals, Applications, and Future Trends." **In Dynamics of Swarm Intelligence Health Analysis for the**

Lead City University Ibadan DO NOT COPY

Next Generation, (2023) 186-209. IGI Global. https://doi.org/10.4018/978-1-6684-6894-4.ch010

Bourian, Imad, Chaimae Elfilali, and Khalid Choughdali. "Enhancing security in intelligent transport system network by integrating blockchain-based smart contracts" **The Journal of Supercomputing,** 81 (13), 2025: 1255. https://doi.org/10.1109/commnet63022.2024.10793370

Bradford, Marianne, and Juan Florin. "Examining the role of innovation diffusion factors on the implementation success of enterprise resource planning systems." **International journal of accounting information systems** 4 (3) (2003): 205-225.

Deng, Shuiguang, Hailiang Zhao, Binbin Huang, Cheng Zhang, Feiyi Chen, Yinuo Deng, Jianwei Yin, Schahram Dustdar, and Albert Y. Zomaya. "Cloud-native computing: A survey from the perspective of services." **Proceedings of the IEEE** 112(1) (2024): 12-46. https://doi.org/10.1109/JPROC.2024.3353855

Dilley, D. U. "Impact of cyberspace on the cybersecurity of critical national assets infrastructures in Nigeria: A review of education and financial sectors." **World Journal of Cybersecurity**. (2022).

Djenna, A., Bodin, U., & Schelen, O. "Attribute-based approaches for secure data sharing in industrial contexts." **IEEE Access**, 11, 2023: 10180–10195. https://doi.org/10.1109/access.2023.3240000

Djenna, A., Harous, S., & Saidouni, D. E. "Internet of things meet the internet of threats: New concern cyber security issues of critical cyber infrastructure." **Applied Sciences**, 11(10), 2021: 4580. https://doi.org/10.3390/app11104580

Dodiya, Kiranbhai Ramabhai, Mukul Jha, and Sammi Jha. "Fortifying the digital forge: unleashing cybersecurity in the interconnected world of digital manufacturing." In Emerging Technologies in Digital Manufacturing and Smart Factories. **IGI Global Scientific Publishing**, 2024. 230-256 https://www.igiglobal.com/chapter/fortifying-the-digitalforge/336132

DoP, Abiodun Adebanjo, Gloria Chigbu, and Christopher M. Osazuwa. "Effect of data protection frameworks against cybercrimes on cyber security in Nigeria." **The American Journal of Political Science Law and Criminology** 6 (9), 2024: 64-84.

Ebeloku, Ademola Iyanda, Adebayo Sulaimon Adeoduy, and James Olalekan Akinbode. "Work Environment and Academic Staff Performance in Federal Polytechnics, South-West, Nigeria." **International Journal of Research and Scientific Innovation**, 2024.

El Sibai, Rayane, Nader Gemayel, Jacques Bou Abdo, and Jacques Demerjian. "A survey on access control mechanisms for cloud computing." **Transactions on Emerging Telecommunications Technologies** 31 (2), 2020: e3720. https://doi.org/10.1002/ett.3720

Lead City University Ibadan DO NOT COPY

Essien, Emmanuel Sunday, and Emmanuel Edun Egbeji. "Digitalizing Cyber Security for Data Management in Higher Education Implication for Educational Management in Nigeria." **J Adv Educ Philos** 8 (4), 2024: 234-238. https://doi.org/10.36348/jaep.2024.v08i04.001

Eze, Udoka Felista, Chukwuemeka Etus, and Joy Ebere Uzukwu. "Database system concepts, implementations and organizations-a detailed survey." **Database** 2 (2), 2014.

Fan Xia, Xiaoyan Wei, Qingyao Zhao, Bo Jin, Zheng Yu, Zhiyong Zha, Dongling Xiao, Fei Long, Geng Wu and Junguo Hu. "Exploration on the Application of Multimodal Biometric Feature Recognition in System Access Control." **IEEE Xplore** 2024. https://doi.org/10.1109/csnt60213.2024.10545831

Farhan, Maruf, Abdul Salih, and Usman Butt. "Enhancing Secure Access and Authorization in Healthcare IoT through an Innovative Framework: Integrating OAuth, DIDs, and VCs." **In Proceedings of the 2023 6th International Conference on Information Science and Systems**, 2023: 254-261. https://doi.org/10.1145/3625156.3625193

Farouk, Suleiman, Chandrashekhar Uppin, and Gilbert George. "Enhancing Cybersecurity in Nigeria: A Proposed Risk Management Framework for Universities." **International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)**, IEEE, 2024: 1-8 https://doi.org/10.1109/seb4sdg60871.2024.10629748

Flynn, Sarah JA. "The records continuum model in context and its implications for archival practice." **Journal of the Society of Archivists** 22 (1), 2001: 79-93.

Garg, V. "Modern Data Governance Technologies and Their Role in Regulatory Compliance: A Study on GDPR and HIPAA". **International Scientific Journal of Engineering and Management**, 03(12), 2024, 1–6. https://doi.org/10.55041/isjem0276

Hoyle, M., and P. Sebina. "Fostering Trust and Transparency in Governance: investigating and addressing the requirements of building integrity in Public Sector Information Systems in the ICT environment: a case of Zambia". **IRMT, London** 2006.

Kayes, A. S. M., Rudri Kalaria, Iqbal H. Sarker, Md Saiful Islam, Paul A. Watters, Alex Ng, Mohammad Hammoudeh, Shahriar Badsha, and Indika Kumara. "A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues." **Sensors** 20 (9), 2020: 2464.

Kemoni, Henry, and Patrick Ngulube. "Relationship between records management, public service delivery and the attainment of the United Nations Millennium Development Goals in Kenya**." Information Development** 24 (4), 2008: 296-306.

Kemoni, Henry. "Theoretical framework and literature review in graduate records management research." **African Journal of Library, Archives and Information Science** 18 (2), 2008: 103-117.

Lead City University Ibadan DO NOT COPY

Krejcie, Robert V, & Daryle, W. *Determining Sample Size for Research Activities*. **University of Minnesota, Duluth & Texas A and M University**, 1970

Kumar, Sunil. "Biometric systems security and privacy issues." **In Leveraging Computer Vision to Biometric Applications**, Chapman and Hall/CRC, 2024: 68-91. https://doi.org/10.1201/9781032614663-4

Laksito, Joni, Berliant Pratiwi, and Widya Ariani. "Harmonizing Data Privacy Frameworks in Artificial Intelligence: Comparative Insights from Asia and Europe." **Perkara: Jurnal Ilmu Hukum dan Politik** 2(4), 2024: 579-588. https://doi.org/10.51903/perkara.v2i4.2229

Li, Jo-Yun, Ruoyu Sun, Weiting Tao, and Yeunjae Lee. "Employee coping with organizational change in the face of a pandemic: The role of transparent internal communication." **Public relations review** 47(1), 2021: 101984. DOI:https://doi.org/10.1016/j.pubrev.2020.101984

Makhura, M., & Du Toit, A. "Records management and Information User behavior at SANParks: A case study. Mousaion," 23 (2), 2007: 213-229.

Malik, Ahmad Kamran, Naina Emmanuel, Sidra Zafar, Hasan Ali Khattak, Basit Raza, Sarmadullah Khan, Ali H. Al-Bayatti, Madini O. Alassafi, Ahmed S. Alfakeeh, and Mohammad A. Alqarni. "*From Conventional to State-of-the-Art IoT Access Control Models*" **Electronics** 9 (10) 2020: 1693. https://doi.org/10.3390/electronics9101693

Manyambula, M. "Records management and accountability." **XIX Bi-Annual ESARBICA General Conference**, Dare es Salaam Tanzania, 2007.

Marquis, Y.A., Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O.O. & Ajayi, S. S. "Proliferation of AI Tools: A multifaceted evaluation of user perceptions and emerging trend." **Asian Journal of Advanced Research and Reports.** Jan. 2024; 18(1):30–35.

Marquis, Yewande Alice. "From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts." **Journal of Engineering Research and Reports** 26 (5), 2024: 138-154. https://www.thedrum.com/news/2 022/05/19/yahoo-lawsuit-allegesemployee-stole-trade-secrets-uponreceiving-trade-desk-job

Marquis, Yewande Alice. "From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts." **Journal of Engineering Research and Reports** 26 (5), 2024: 138-154.

Marshall, Peter. "Life Cycle Versus Continuum: What is the Difference?" **Informaa Quarterly** 16 (2), 2000: 20-25.

Mnjama, Nathan, and Justus Wamukoya. "E-government and records management: an assessment tool for e-records readiness in government." **The Electronic Library** 25(3), 2007: 274-284. DOI:https://doi.org/10.9734/ajrcos/2024/v1 7i5442

Lead City University Ibadan DO NOT COPY

Naboth-Odums, Augustine, Friday Ekahe Abanyam, Abdulrahman Abdulkadir, and Victor Attah Abanyam. "Information and Security Control Mechanisms Embraced for Effective Information Management in Colleges of Education in Nigeria." **Golden Ratio of Social Science and Education** 2 (2), 2022: 98-111.

Njoku, D. O., Nwokorie, E. C., Okolie, S. A., & Odii, J. N. "Cyberspace Activities Awareness and Security Strategies in Tertiary Institutions in Nigeria." **Journal of Cyber Security**, 3(2), 2019: 439–445. https://irejournals.com/formatedpaper/1701507.pdf

Nowrozy, Raza, Khandakar Ahmed, Hua Wang, and Timothy Mcintosh. "Towards a universal privacy model for electronic health record systems: an ontology and machine learning approach." **MDPI in Informatics**, 10 (3), 2023: 60 MDPI, DOI:https://doi.org/10.3390/informatics100 30060

Nte, Ngboawaji Daniel, Vigo Augustine Teru, and Arifin Ridwan. "Challenges of information security laws and legislations in Nigeria's institutions of higher education: Views from Yola, Adamawa state." **Research and Development in Education (RaDEn)** 4 (2), 2024: 1498-1519. https://doi.org/10.22219/raden.v4i2.35711

Nyame, Gabriel, and Zhiguang Qin. "Precursors of role-based access control design in KMS: A conceptual framework." Information 11 (6), 2020: 334. https://doi.org/10.3390/info11060334

Oguguo, Basil CE, and Christopher A. Ocheni. "Cybersecurity: a tool for curbing examination breaches and improvement of the quality of large-scale educational assessments." **Information Security Journal**: A Global Perspective 33 (4), 2024: 359-373. https://doi.org/10.1080/19393555.2023.2284761

Okokpujie, Kennedy, Chinyere G. Kennedy, Kamsiyochukwu Nnodu, and Etinose Noma-Osaghae. "Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University)." **International Journal of Sustainable Development & Planning** 18 (1), 2023. https://doi.org/10.18280/ijsdp.180127

Olabanji, S. O. "AI for identity and access management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems." **Asian Journal of Research in Computer Science**, 17(3), 2024: 38–56. https://doi.org/10.9734/ajrcos/2024/v17i3423

Olabanji, Samuel Oladiipo, Oluseun Babatunde Oladoyinbo, Christopher Uzoma Asonze, Tunboson Oyewale Oladoyinbo, Samson Abidemi Ajayi, and Oluwaseun Oladeji Olaniyi. "Effect of adopting AI to explore big data on personally identifiable information (PII) for financial and economic data transformation." **Asian Journal of Economics, Business and Accounting** Available at SSRN 4739227 (2024). DOI: https://doi.org/10.9734/ajeba/2024/v24 i41268

Lead City University Ibadan DO NOT COPY

Olabanji, Samuel Oladiipo, Oluwaseun Oladeji Olaniyi, Chinasa Susan Adigwe, Olalekan J. Okunleye, and Tunboson Oyewale Oladoyinbo. "AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems." Authorization, and Access Control within Cloud-Based Systems **Asian Journal of Research in Computer Science.** (2024). DOI: https://doi.org/10.9734/ajrcos/2024/v1 7i3423

Olabanji, Samuel Oladiipo, Tunboson Oyewale Oladoyinbo, Christopher Uzoma Asonze, Chinasa Susan Adigwe, Olalekan J. Okunleye, and Oluwaseun Oladeji Olaniyi. "Leveraging fintech compliance to mitigate cryptocurrency volatility for secure us employee retirement benefits: Bitcoin ETF case study." **Asian Journal of Economics, Business and Accounting** Available at SSRN 4739190 (2024).

Olabanji, Samuel Oladiipo, Yewande Marquis, Chinasa Susan Adigwe, Samson Abidemi Ajayi, Tunboson Oyewale Oladoyinbo, and Oluwaseun Oladeji Olaniyi. "AI-driven cloud security: Examining the impact of user behavior analysis on threat detection." **Asian Journal of Research in Computer Science** 17 (3), 2024: 57-74. https://doi.org/10.9734/ajrcos/2024/v1 7i3424

Oladokun, Bolaji, Emmanuel Oloniruha, Deborah Mazah, and Obediah Okechukwu. "Cybersecurity Risks: A Sine Qua Non for University Libraries in Africa." **Southern African Journal of Security** 2, 2024: 1-14. https://doi.org/10.25159/3005-4222/15320

Oladoyinbo, Tunboson Oyewale, Samuel Oladiipo Olabanji, Oluwaseun Oladeji Olaniyi, Olubukola Omolara Adebiyi, Olalekan J. Okunleye, and Adegbenga Ismaila Alao. "Exploring the challenges of artificial intelligence in data integrity and its influence on social dynamics." **Asian Journal of Advanced Research and Reports** 18 (2), 2024: 1-23. DOI: https://doi.org/10.9734/ajarr/2024/v18i 2601

Olabanji, Samuel Oladiipo, Yewande Marquis, Chinasa Susan Adigwe, Samson Abidemi Ajayi, Tunboson Oyewale Oladoyinbo, and Oluwaseun Oladeji Olaniyi. "AI-driven cloud security: Examining the impact of user behavior analysis on threat detection." **Asian Journal of Research in Computer Science** 17 (3), 2024: 57-74.

Olabanji, Samuel Oladiipo, Oluseun Babatunde Oladoyinbo, Christopher Uzoma Asonze, Tunboson Oyewale Oladoyinbo, Samson Abidemi Ajayi, and Oluwaseun Oladeji Olaniyi. "Effect of adopting AI to explore big data on personally identifiable information (PII) for financial and economic data transformation." Available at **SSRN** 4739227 (2024).

Oladoyinbo, Tunboson Oyewale, Samuel Oladiipo Olabanji, Oluwaseun Oladeji Olaniyi, Olubukola Omolara Adebiyi, Olalekan J. Okunleye, and Adegbenga Ismaila Alao. "Exploring the challenges of artificial intelligence in data integrity and its influence on social dynamics." **Asian Journal of Advanced Research and Reports** 18 (2), 2024: 1-23.

Lead City University Ibadan DO NOT COPY

Olaniyi, Oluwaseun Oladeji, Jennifer Chinelo Ugonnia, Folashade Gloria Olaniyi, Aisha Temitope Arigbabu, and Chinasa Susan Adigwe. "Digital collaborative tools, strategic communication, and social capital: Unveiling the impact of digital transformation on organizational dynamics." **Asian Journal of Research in Computer Science** 17 (5), 2024: 140-156. DOI:https://doi.org/10.9734/ajrcos/2024/v1 7i5444

Olaniyi, Oluwaseun Oladeji. "Best practices to encourage girls' education in maiha local government area of adamawa state in Nigeria." **The University of Arkansas Clinton School of Public Service. Research Gate** Available at SSRN 4564307 (2021). DOI: https://doi.org/10.13140/RG.2.2.26144 .25606

Omotunde, Habeeb, and Maryam Ahmed. "A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond." **Mesopotamian Journal of CyberSecurity** (2023): 115-133. DOI:https://doi.org/10.58496/MJCSC/2023/ 016.

Pal, Shantanu, and Zahra Jadidi. "Protocol-based and hybrid access control for the iot: Approaches and research opportunities." **Sensors Journal** 21 (20), 2021: 6832. DOI: https://doi.org/10.3390/s21206832

Park, Jaehong, Ravi Sandhu, Maanak Gupta, and Smriti Bhatt. "Activity control design principles: Next generation access control for smart and collaborative systems." **IEEE Access** 9, 2021: 151004-151022. DOI:https://doi.org/10.1109/access.2021.3 126201

Parkinson, Simon, and Saad Khan. "A survey on empirical security analysis of access-control systems: a real-world perspective." **ACM Computing Surveys** 55 (6), 2022: 1-28. DOI: https://doi.org/10.1145/3533703

Prabhu, Sunitha, and Nik Thompson. "A primer on insider threats in cybersecurity." **Information Security Journal**: A Global Perspective 31 (5), 2022: 602-611. DOI: https://doi.org/10.1080/19393555.202 1.1971802

Pundlik M. & Jadhav P.P. “Block chain technology in healthcare system for sharing confidential information between departments and doctors.” **International Journal of Intelligent Systems and Applications in Engineering**. 12(12s), 2024:01-10. https://ijisae.org/index.php/IJISA E/article/view/4488

Putch, K. “Healthcare security services firms tackle ransomware spike.” **TechTarget**. 2021. https://www.techtarget.com/searchitchannel/feature/Healthcare-security-services-firms-tackle-ransomware-spike?bucket=NEWS&topic=299987

Quadri, Faruq, Oluwaseun Oladeji Olaniyi, and Olugbenga O. Olaoye. "Interplay of Islam and economic growth: Unveiling the long-run dynamics in Muslim and Non-Muslim countries." **Asian journal of education and social studies** 49 (4), 2023: 483-498. DOI: https://doi.org/10.9734/ajess/2023/v49 i41226

Ragothaman, Kaushik, Yong Wang, Bhaskar Rimal, and Mark Lawrence. "Access control for IoT: A survey of existing research, dynamic policies and future directions." **Sensors** 23 (4), 2023: 1805. https://doi.org/10.3390/s23041805

LeadCity University Ibadan DO NOT COPY

Rao, K. Rajesh, Ashalatha Nayak, Indranil Ghosh Ray, Yogachandran Rahulamathavan, and Muttukrishnan Rajarajan. "Role recommender-RBAC: Optimizing user-role assignments in RBAC." **Computer Communications** 166, 2021: 140-153.

Rauf, Usman, Mohamed Shehab, Nafees Qamar, and Sheema Sameen. "Formal approach to thwart against insider attacks: A bio-inspired auto-resilient policy regulation framework." **Future Generation Computer Systems** 117, 2021: 412-425.

Raymond, Anjanette H. "Data management regulation: Your company needs an up-to-date data/information management policy." **Business Horizons** 56 (4), 2013: 513-520. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265560

Saxena, Neetesh, Emma Hayes, Elisa Bertino, Patrick Ojo, Kim-Kwang Raymond Choo, and Pete Burnap. "Impact and key challenges of insider threats on organizations and critical businesses." **Electronics** 9 (9), 2020: 1460. https://doi.org/10.3390/electronics909 1460.

Science Direct, Access Control Policies, **Science Direct Journals**, https://www.sciencedirect.com/topics/computer-science/access-control-policies

Sejane, L. "Records Management in Africa: three case studies and a proposal. In Information 2000: a version for the SCECSAL region". **Proceedings of the 14th Conference of Eastern, Central and Southern African Libraries**, 2005, Windhoek, Namibia.

Seshagirirao, V.K.A. & Babatope, A.B. "Data privacy, security, and governance: A global comparative analysis of regulatory compliance and technological innovation." **Global Journal of Engineering and Technology Advances,** 21(3), 2024, 190–202. https://doi.org/10.30574/gjeta.2024.21.3.0246

Shah, Wasim Fathima. "Preserving privacy and security: a comparative study of Health Data regulations-GDPR vs. HIPAA." **Int. J. Res. Appl. Sci. Eng. Technol** 11 (8), 2023: 2189-2199. https://doi.org/10.22214/ijraset.2023.55551

Siedlecki, Sandra L. "*Understanding descriptive research designs and methods."* **Clinical Nurse Specialist** 34 (1), 2020: 8-12.

Taranto-Vera, Gilda, Purificación Galindo-Villardón, Javier Merchán-Sánchez-Jara, Julio Salazar-Pozo, Alex Moreno-Salazar, and Vanessa Salazar-Villalva. "Algorithms and software for data mining and machine learning: a critical comparative view from a systematic review of the literature." **The Journal of Supercomputing** 77 (10), 2021: 11481-11513. DOI:https://doi.org/10.1007/s11227-021- 03708-5

Teimoor, Ramyar Abdulrahman. "A review of database security concepts, risks, and problems." **UHD Journal of Science and Technology** 5 (2), 2021: 38-46. https://doi.org/10.21928/uhdjst.v5n2y2021

Tomar, Manish, and Jawaharbabu Jeyaraman. "Reference data management: A cornerstone of financial data integrity." **Journal of Knowledge Learning and Science Technology**

Lead City University Ibadan DO NOT COPY

ISSN: 2959-6386, 2 (1), 2023: 137-144. DOI:https://doi.org/10.60087/jklst.vol2.n1.p144.

Trabelsi, Rahma, Ghofrane Fersi, and Mohamed Jmaiel. "Access control in Internet of Things: A survey." **Journal of Computers & Security** 135 (2023): 103472. https://doi.org/10.1016/j.cose.2023.103472

Urbanus, BILLE David. "Impact of cyberspace on the cybersecurity of critical national assets infrastructures in Nigeria: A review of education and financial sectors." **World Journal of Advanced Research and Reviews** 16 (1), 2022: 595-604. https://doi.org/10.30574/wjarr.2022.16.1.1057

Yang, Benyuan. "Enforcement of separation of duty constraints in attribute-based access control." **Computers & Security** 131 (2023): 103294. DOI:https://doi.org/10.1016/j.cose.2023.10 3294

Zaidi, Tanzeel, Muhammad Usman, Muhammad Umar Aftab, Hanan Aljuaid, and Yazeed Yasin Ghadi. "Fabrication of flexible role-based access control based on blockchain for internet of things use cases." **IEEE Access** 11 (2023): 106315-106333.

Zubair, Maria, Maryam Sabzevari, Vikramajeet Khatri, Sasu Tarkoma, and Kimmo Hätönen. "Access control for trusted data sharing." **EURASIP Journal on Information Security** 2024, no. 1 (2024):30. https://doi.org/10.1186/s13635-024-00178-z

Reports and Organizational Publications

Computer Security Division. (2016). Role Engineering and RBAC Standards - Role Based Access Control. CSRC, NIST. Available: https://csrc.nist.gov/projects/rolebased-access-control/role-engineeringand-rbac-standards (accessed Mar. 30, 2024).

GAO. (2002). Information Management: Challenges in Managing and Preserving Electronic Records; Report to Congress Requesters. GAO, USA.

IRMT. (2009). Managing Personnel Records in an Electronic Environment: TERM Project. IRMT, London. Available at: www.irmt.org (accessed July 16, 2009).

Glover, Claudia. "Pegasus Airline Breach Sees 6.5 TB of Data Left in Unsecured AWS Bucket." TechMonitor30 (2022). https://techmonitor.ai/technology/cybersecurity/pegasus-airline-data-breachaws-bucket

International Comparative Legal Guides (ICLG). Data Protection Laws and Regulations: Nigeria, 2024, 2024–2025. https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria#:~:text=The%20Nigeria%20Data%20Protection%20Commission%20%28%E2%80%9CNDPC%E2%80%9D%29%20is%20the,NDPA%20in%20Nigeria.%20The%20NDPA%20establishes%20the%20NDPC

Lead City University Ibadan DO NOT COPY

Royal College of Arts, Information Handling Policy, Dec. 2024, https://www.rca.ac.uk/more/organisation/policies-and-codes-of-practice/information-handling-policy

Web Sources and Blogs

Paganini, P. (2022). Block discloses data breach involving cash app potentially impacting 8.2 million US customers. Security Affairs. Available: https://securityaffairs.com/129892/data-breach/block-cash-app-data-breach.html (accessed Mar. 14, 2024).

Glover, Claudia. "Pegasus Airline Breach Sees 6.5 TB of Data Left in Unsecured AWS Bucket." TechMonitor30 (2022). https://techmonitor.ai/technology/cybersecurity/pegasus-airline-data-breachaws-bucket

International Comparative Legal Guides (ICLG). (2024). Data Protection Laws and Regulations: Nigeria. Available: https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria.

Science Direct, Access Control Policies, **Science Direct Journals**, https://www.sciencedirect.com/topics/computer-science/access-control-policies

Lead City University Ibadan DO NOT COPY

Appendices

Questionnaire

Lead City University

Faculty of Communication and Information Sciences (FCIS)

Department of Information Management

Dear Respondent,

I am a Master's student of the above-named institution, gathering data for academic research on the topic "Data Handling Stages, Access Control and Information Security Practice among Non-Academic Staff in State-owned Polytechnics, Oyo State, Nigeria. To achieve this, your optimum cooperation is needed; there are no right or wrong answers. All your responses will be kept confidential and used for research purposes only.

Thank you.

Researcher

Lead City University Ibadan DO NOT COPY

SECTION A: DEMOGRAPHIC INFORMATION

Gender: Male ( ), Female ( )

Age: 20 – 25 ( ), 26 – 30 ( ), 31 – 35 ( ), 36 – 40 ( ), 41-45 ( ), 46 and above ( )

Educational Level: NCE ( ) Bachelor's degree ( ) Master's degree ( ) Ph.D ( )

Years of experience: 5 – 10 ( ), 11 – 15 ( ), 16 – 20 ( ), 21 – 25 ( ), 26 - 30 ( )

SECTION B: Level of Information Security of Non-Academic Staff in Oyo State-owned Polytechnics

The statement in this section assesses the level of information security practice by Non-Academic Staff in Oyo State-owned Polytechnics. Using the four-point Likert scale provided below. Please tick the appropriate choice that indicates your opinion on level of information security in your institution.

Very High (VH) = 4, High (H) =3, Low (L) =2, Very Low (VL) =1

S/N	At what level have you engaged in the following?	VH 4	H 3	L 2	VL 1
	Information Confidentiality				
1	Acceptance guidelines for new information security				
2	Existence of a network operational guideline in your organization				
3	Identification of information security features				
4	Protection of system documentation against unauthorized access				
5	Establishment of information exchange policy in your organization				
	Information Integrity				
6	Separation of the development of operational facilities				
7	Existence of a policy prohibiting the use of unauthorized software in your organization				
8	Backup policy for information				
9	Policy to protect the electronic distribution of information				
10	Procedures to monitor system use				
	Information Availability				
11	Procedures for handling and storing information				
12	Existence of a guideline for physical media in transit that contains information				
13	The activities of system administrators and system operators are being logged				
14	Employees' activities are monitored under the existing legal framework				
15	Monitoring the use of resources in computer systems is performed				

SECTION C: Data Handling Stages in Oyo State-owned Polytechnics

Lead City University Ibadan DO NOT COPY

The statement in this section examines the data handling stages that exists in Oyo State-owned Polytechnics. Using the four-point Likert scale provided below. Please tick the appropriate choice that indicates your opinion on the data handling stages in your Polytechnic.

Strongly Agreed (SA) = 4, Agreed (A) =3, Disagreed (D) =2, Strongly Disagreed (SD) =1

S/N	What is your agreement with the following?	SA 4	A 3	D 2	SD 1
	Data Creation				
1	Process of documenting academic data				
2	Existence of a license that describes how data is used				
3	Filing plans are created to least primary data used by functional units				
	Data Classification				
4	Process for archiving data in a repository for long-term storage				
5	Practice of assigning a permanent identifier to your datasets				
6	Data created by you is appropriately cited				
	Data Scheduling and Maintenance				
7	Inclusion of a data availability statement in your manuscripts				
8	Documenting data for easy understanding				
9	Data retention schedule is in place				
	Use of Information				
10	The institution addresses data privacy and security issues				
11	Evaluating the credibility of information sources				
12	Information verification before using for your decision-making				

Lead City University Ibadan DO NOT COPY

SECTION D: Access Control in the Oyo State-owned Polytechnics

The statement in this section identify the level of access control by registry of staff of Oyo State-owned Polytechnics. Using the four-point Likert Scale provided below. Pleases tick the appropriate choice that indicates your opinion.

Very High (VH) = 4, High (H) =3, Low (L) =2, Very Low (VL) =1

S/N	What is your level of access control of data in your institution?	VH 4	H 3	L 2	VL 1
	Roles Definition				
1	Mode of equipment identification				
2	Separation of data networks into domains according to its function				
3	Routing implementation to enforce access control policy				
	Permissions Allocation Control				
4	User password guideline control				
5	Periodic review of user access rights				
6	User guideline for the usage of passwords				
	Sessions Management				
7	Clear desk and screen policy				
8	Existence of policies for the use of data network services				
9	Authentication of remote users				
	User Assignments Control				
10	Restriction on users' ability to connect to data network				
11	Incorporating users authentication for access to institution information system				
12	Understanding time frame for connecting to information system				

Lead City University Ibadan DO NOT COPY

Bio Data

A. PERSONAL DATA

1. **Title:** Mr.
2. **Full Name:** Ibrahim Sunday **Oyekola**
3. **Date of Birth:** 27th August, 1995

4. **Nationality/State of Origin:** Nigeria/Oyo State
5. **Marital Status:** Married
6. **Number and Ages of Children:** 1| 2years
7. **Phone No:** +234 8101970233
8. **Email Address:** oyekolakanmi@gmail.com | oyekola.ibrahim@polyibadan.edu.ng
9. **Faculty:** Business and Communication Studies
10. **Department:** Office Technology and Management

B. QUALIFICATIONS AND EXPERIENCE

1. School/Institutions Attended with Dates and Qualification:

- Lead City University (M.Sc.) In view
- Lead City University (BSc.) 2021 - 2023
- The Polytechnic, Ibadan (Higher National Diploma) 2016 - 2018
- The Polytechnic, Ibadan (National Diploma) 2013 - 2015
- Renascent High School 2005 - 2011
- Ratibi Muslim School 1997 - 2005

2. Academic and Professional Qualifications

- Masters of Science, *Office & Info. Mgt.* In View
- Bachelor of Science, *Office & Info. Mgt.* (First Class Honors) 2023
- Higher National Diploma, *Office Tech. and Mgt.* (Upper Credit) 2018
- National Diploma, *Office Tech. and Mgt.* (Upper Credit) 2015
- Secondary School Leaving 2011
- First School Leaving 2005

3. Membership of Professional Bodies

- Nigerian Institute of Management (Graduate Member *'ID258556'*) 2021
- National Institute of Office Administrators and Information Managers(NIOAIM) 2021
- National Institute of Office Technology and Information Managers (NIOTIM) 2025
- Chartered Institute of Information and Strategy Management (CIISM) 2025

4. Work Experience

i. Teaching Experience (Employer, Address/Designation/Subject Taught/Date

Employer: The Polytechnic, Ibadan
Address: Sango Eleyele Road, Department of Office Technology and Mgt.
Designation: Lecturer **Date:** 2023

Employer: Community Secondary School
Address: Anong Bahumono Community, Abi LGA, Cross River State
Designation: Teacher **Date:** 2019

ii. Professional Work Experience

- Certified in all Ms Office Applications (The Polytechnic, Ibadan) 2018
- Computer Training Certificate (Home Flo Computer Centre) 2011

iii. Administrative Work Experience

The Polytechnic, Ibadan, Exams and Record Unit Technical Officer 2023

Lead City University Ibadan DO NOT COPY

The Polytechnic, Ibadan, Faculty of Business and Communication Studies	Data Entry Officer	2022
The Polytechnic, Ibadan, Open Distance Flexible and e-Learning Centre (ODFeL)	Technical Officer	2022
The Polytechnic, Ibadan, Centre for Information and Data Management Unit (CIDM)	Data Entry Officer	2020-2022
Community Secondary School Anong, Abi, Cross River State (National Youth Service)	Teacher	2019-2020
The Polytechnic, Ibadan, Accountancy Department	Secretary	2019
The Polytechnic, Ibadan, Junior Staff Estab. Unit (Registry)	Secretary	2016-2019
The Polytechnic, Ibadan, Deputy Registrar, Personnel (Industrial Training)	Secretary	2015-2016

C. RESEARCH/ PROJECT/INTERVENTION/INNOVATION/DESIGN

1. **Research in progress/brief description (if any with dates) :** Nil
2. **Project/invention etc/completed but not yet patented with dates:** Nil
3. **Publications/Exhibition/Designs/Give details of books and articles stating Extract references in chronological order:** Nil
4. **Dissertation or Thesis**
   - Data Handling Policy, Access Control and Information Security among Registry Staff in Oyo State-Owned Polytechnics (**MSc. Thesis *in progress)***
5. **Books or Monographs:** Nil
6. **Published Articles:**

Waheed, B. A., Ajayi, J. M., **Oyekola, I. S.**, Adeyinka, M. G., Agbejule, O., Adewale, M. M., & Windapo, T. O. (2024). *Impact of information management on office managers' job performance in a digitalised office (A study of University of Ibadan, Ibadan, Oyo State).* In T. E. Adenekan, G. E. Oyedokun, & O. J. Ige (Eds.), Proceedings of the 2nd National Institute of Office Administrators and Information Managers (NIOAIM) Biennial Conference, Themed: Office administration and information management in the digital era (pp. 350–365). National Institute of Office Administrators and Information Managers. ISBN 978-978-766-2298

Oyekola, I. S., & Adewale, M. M. (2025). *Artificial Intelligence and Machine Ethics in Office Information Security.* In a Festschrift in hornor of Prof. Eseza Akior Erwat, titled; Efficiency Unveiling: A Festschrift of Administration, Office and Information Management System (pp. 363-370). Department of Information Management, Lead City University, Ibadan, Oyo State, Nigeria. ISBN 978-978-697-535-1

Oguntayo, O. O., Waheed, B. A., Fasipe, O. O., **& Oyekola, I. S.** (2025). *Leveraging data-driven decision-making for enhancing office management efficiency: Innovation and best practices* [Conference presentation]. 1st International Conference, Themed; Navigating the Future: Innovation in the Field of Information Management, Department of Information Management, Lead City University, Ibadan, Nigeria.

Lead City University Ibadan DO NOT COPY

7. **Papers already accepted for publication (*please attach copy of paper)*:**
   Oyekola, I.S., & T.E Adenekan (2025) *Data Handling Stages, and Information Security Practice among Non-Academic Staff in State-Owned Polytechnics, Oyo State, Nigeria.* (Submitted for publication)

8. **Exhibitions/Designs/Project/Invention etc:** Nil
9. **Other works of relevance**
   Oyekola, I.S. (2015). *Impact of Information and Communication Technology (ICT) on the Running of Management Information System in Tertiary Institutions, A Case Study of University of Ibadan* (ND Project "n*ot published"*)

   Oyekola, I.S. (2018). *The effect of Office Equipment Maintenance in an organization* (Seminar Paper "n*ot published"*).

   Oyekola, I.S. (2018). *Office Equipment and Maintenance as a Panacea to Secretary Administrative Efficiency in an Organization, A Case Study of University of Ibadan* (HND Project Research "n*ot published"*)

   Oyekola, I.S. (2021). *The Nigeria history, Ethnic groups, Food, Clothing and Culture*. Being a presentation made at a meet and greet session with a Rotaract club in India ("n*ot published"*)

   Oyekola, I.S., Aromona, K.O & Olatunji, D.A. (2023). *Electronic Record Management Practices and Effective Job Performance of Administrative Personnel in The Polytechnic, Ibadan* (BSc. Project *"*n*ot published"*)

   Oyekola, I.S. (2024) *Influence of Record Management Practices on Effective Job Performance of Secretaries in The Polytechnic, Ibadan.* Being a Conference Paper presented at The Polytechnic, Ibadan, Faculty of Business and Communication Studies Annual Conference, Themed: Managing Change for Sustainable Development in Nigeria (2024, 4th-5th June).

   Oyekola, I.S., & R.E Ajibola & Hammed, S.O., (2025) *Artificial Intelligence and Academic Performance of Office Technology and Management Students in Polytechnics in Nigeria.* Being Being a Conference Paper presented at Faculty of Social Management and Humanities, The Polytechnic, Ibadan 2025 National Conference Themed: Exploring the Impact of Artificial Intelligence on Social Structures, Human Relationship, Cultural Norms and the Environment in Nigeria (October 6th-10th, 2025)

   Oyekola, I.S., & T.E Adenekan (2025) *Data Handling Policy, Access Control and Information Security among Registry Staff in Oyo State-Owned Polytechnics (MSc. Thesis in progress)*
10. **Conferences, workshops attended with venue, date and paper presented (if any)**
    - Faculty of Social Management and Humanities, The Polytechnic, Ibadan 2025 National Conference Themed: Exploring the Impact of Artificial Intelligence on Social Structures, Human Relationship, Cultural Norms and the Environment in Nigeria (October 6th-10th, 2025)
    - Department of Information and Management 1st international conference (2025).

Lead City University Ibadan DO NOT COPY

- Faculty of Business and Communication Studies, The Polytechnic, Ibadan Annual Conference (2024, 4th-5th June), Themed: Managing Change for Sustainable Development in Nigeria.
- National Institute of Office Administrators and Information Managers (NIOAIM) 2nd Biennial Conference, Themed: Office administration and information management in the digital era (April 16th-17th, 2024).
- Assistant Trainer at a six (6) days Seminar on Intermediate Microsoft Office Packages organized by Oyo State Government at Ibadan Business School (2022).
- National Institute of Office Administrators and Information Managers (NIOAIM) 2022 Conference Tagged "Repositioning Office Administration and Information Management for Innovation, Sustainability Development and Global Competitiveness) on 8th February, 2022.
- Assistant Trainer at a three (3) days Seminar on Basic Microsoft Office Packages organized by Oyo State Government at Ibadan Business School (2020).
- Registry Conference on "Team Work in an Organization", Registry Department, The Polytechnic, Ibadan (2017).
- Office Technology and Management Curriculum and Challenges of 21st Century Office organized by Business and Office Administrators of Nigeria in collaboration with Department of Office Technology and Management, The Polytechnic, Ibadan (2016).

D. Extra-Curricular Activities:

1. Within the Institution

- Class Coordinator
- Project Supervisor
- Departmental examination officer
- Member, Faculty of Business and Communication Studies Committee on Fuji Documentary Screening
- Member, Faculty of Business and Communication Studies Dean's Special Duties Committee

2. Outside the Institution

- BOD Member, Rotaract Club eClub of Ibadan Pacesetter
- Member, Rotary International District 9126, Zone 2, Nigeria
- Class Representative, 2024/2025 M.Sc. Students, Department of Office and Information Management, Lead City University, Ibadan, Oyo State

Signature **Date**

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

University Compliance Certification

This is to certify that this thesis by Ibrahim Sunday OYEKOLA with matriculation number: LCU/PG/006349, in the Department of Information Management, Faculty of Communication and Information Science, Lead City University, Ibadan, is in FULL compliance with the approved university format and style.

Lead City University Ibadan DO NOT COPY

Signature	**Date**