UKR Journal of Multidisciplinary Studies (UKRJMS)
Homepage: https://ukrpublisher.com/ukrjms/
Email: submit.ukrpublisher@gmail.com
Volume 2, Issue 6, 2026
ISSN: 3049-432X (Online)
OPEN ACCESS

A Comprehensive Data Protection Framework for Securing University ICT Infrastructure and Digital Assets

Ojo Stephen Aderibigbe[1]*, Giyas Olalekan Apenna[2] and Adewale Abdulrazaq Shomope[3]

[1,2,3]Department of Computer Sciences, Lagos State University of Science and Technology, Ikorodu, Lagos State, Nigeria.

***Corresponding Author**: Ojo Stephen Aderibigbe

DOI: *https://doi.org/10.5281/zenodo.20823927*

Article History

Original Research Article

Received: 20-04-2026

Accepted: 28-05-2026

Published: 24-06-2026

Citation: Ojo Stephen Aderibigbe, Giyas Olalekan Apenna & Adewale Abdulrazaq Shomope. (2026). A Comprehensive Data Protection Framework for Securing University ICT Infrastructure and Digital Assets. UKR Journal of Multidisciplinary Studies (UKRJMS), 2(6), 291-301.

Abstract

With the fast digital transformation of higher education institutions and the use of online learning platforms, University ICT centres have to deal with a significant amount of sensitive data, raising significant privacy and cybersecurity issues. This paper discusses the design, deployment and evaluation of a Data Protection Framework (DPF) for the ICT Centre of Lagos State University of Science and Technology (LASUSTECH). A vulnerability assessment was carried out using a design science research approach to identify the major security risks, such as weak access controls, unencrypted devices, cloud storage vulnerabilities, threats from removable media, and password-based attacks. The proposed framework integrates four key components: access control, data encryption and backup, auditing and compliance, and incident response and training. Security mechanisms include Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Biometric Access Control, AES-256 encryption, secured backup and recovery procedures in line with Nigeria Data Protection Act (2023), NDPR and ISO/IEC 27001 standards. The evaluation results indicated 75% reduction in unauthorized access attempts, 91% of staff adopting MFA, incident response time from 24 hours to less than 6 hours and an increase in cybersecurity awareness participation from 42% to 86%. This framework improves data protection, compliance, institutional resilience, and stakeholder confidence and provides a scalable model for higher education institutions.

Keywords: *Data Privacy, Data Security Framework, Higher Education Institutions, Role-Based Access Control, Multi-Factor Authentication.*

1.0 Introduction

University Information and Communication Technology (ICT) Centres are in a unique position as they manage, protect, and administer crucial institutional information such as student records, research outputs, financial documents, administrative databases etc. As facilitators of key digital services, such centres must put in place measures to ensure their systems do not allow unauthorised access or spread software products that are harmful (Ngwenya & Ngoepe, 2020). While the need for operational efficiency mandates ICT centres, they must also comply with basic information security tenets of confidentiality, integrity and availability because all three are essential characteristics of a secure information management model (Chaurasia & Kumar, 2023). The extensive amount of personal and institutional data represents an attractive target for cybercriminals, contributing to the growing digitization of academic processes. Student identification details, staff records, research results and intellectual property assets are also valuable targets for cyberattacks (Arina 2022) such as phishing schemes and other forms of cyber exploitation. Moreover, both internal and external threat actors can target privacy, information systems changed or destroyed and targeting internet-based services. Of these threats, insiders tend to represent a greater risk due to their privileged access to institutional resources. As the need for robust mechanisms to protect one owners' data continues to grow, on 14 July, the Nigerian government passed into law the Nigeria Data Protection Act 2023 (the "NDPA"), a comparatively exhaustive blue print of

legislation for purposes of personal information protection and lawful treatment. It's also responsible for overseeing compliance with the legislation and regulating these data-processing activities, through a recently established Nigeria Data Protection Commission. The Act is structured to promote practices that strengthen privacy and information security while requiring personal data be collected, processed, and stored more fairly. It also aims at protecting the data subject rights by means of legal protection, remedy and redress when such rights are undermined or violated. To ensure this data's confidentiality, integrity, and availability, it is imperative to establish a robust Data Protection Framework (DPF) for institutional ICT centers. The University ICT center has witnessed significant improvement in its operations. However, with these improvements there are vulnerabilities that expose the institution to security threat and privacy breaches. The ICT center is tasked with ensuring the security and efficiency of digital operations, making it making it imperative to adopt a framework that will ensure privacy and data security. For LASUSTECH, a rapidly evolving institution, there is a need for a robust Data Protection Framework. This is necessary so as to safeguard its digital assets and maintain stakeholder trust. This work assesses the current data privacy and security practices at LASUSTECH ICT center, propose a comprehensive framework for privacy and data protection, and ensure compliance with National Data Protection policy. This work explores the design and deployment of a DPF for LASUSTECH ICT Center. It outlines the framework's components, implementation strategies, and alignment with international best practices. The objectives are to mitigate security risks, enhance operational efficiency, and ensure compliance with data protection regulations (ISO/IEC, 2013).

2.0 Literature Review

The digital age has created transformative opportunities for higher education institutions, revolutionizing how knowledge is shared, accessed, and absorbed (Siphambili, 2024**)**. The increasing reliance on Information and Communication Technology (ICT) in higher education Higher education institutions have seen a swift uptick in the use of digital technologies, which has led to burgeoning needs for data protection and information security systems. The ICT centres in the university are custodians of all major information, which involves record-keeping and transaction of sensitive data including student achievement, research outputs, personnel information and transactions. Due to the hundreds of terabytes of data containing valuable research and multiple personally identifiable information stored in their information systems, academic institutions have become very attractive targets for cybercriminals and hacktivist groups in recent years. Moreover, the university environment characterized by constant intake and turnover of students and staff, coupled with shortages in permanent ICT staff at some universities, increases vulnerability to information security breaches. This can be the Foundation for Improving Cyber Security-Operational, Technical and managerial controls to Protect information Assets against threats. To ensure information security, NIST SP 800-12r1 defines the protection of information and information systems, which provides a list of controls that support the development of secure and resilient information systems. These controls are the operational, technical, and management standards and guidelines that information systems use to maintain confidentiality, integrity, and availability. These controls really serve to preserve the three (3) main priorities of information security also called as CIA triad which is Confidentiality, Integrity and Availability. In this model, authentication is the process of verifying a person before allowing them access to system resources. While authorization determines which specific privileges and services an authenticated user should have post-authentication Confidentiality is the protection of information from being accessed by unauthorized individuals, ensuring that data is revealed only to those with appropriate permissions (Serb et al, 2013; Adams & Blandford, 2003). Effectively, it protects against unauthorized access or abuse of information. Accountability, in contrast, refers to the mechanisms for auditing and billing user activities or resource utilization (Song et al., 2013). Higher education institutions have some of the largest and most diverse user populations in any sector, making a security framework necessary to protect its data; both institutional information and personal information. As a result, security mechanisms including authentication protocols, encryption technologies and others protective controls are regularly implemented to improve privacy protection and protect the digital assets. Globally, Universities' digital transformation has been rapid, with ICTs at its core and wielding their influence, enhancing learning, streamlining administrative processes for good, and promoting research (Ulven & Wangen, 2021). However, this progress exposes institutions to a spectrum of internal and external cyber threats. As Lallie *et al.* (2023) note, the sensitive data held by Universities (e.g., student records, research

outputs, financial information, etc) makes them lucrative targets for cybercriminals and hacktivists. Internal threats, such as inadvertent breaches by staff or students, also pose significant challenges. Lallie *et al.* (2023), Identifies Universities as a high-risk due to decentralized data management. There is also issues of trust erosion caused by fragmented governance and limited user awareness (Manda, 2021). Furthermore, Sun *et al.* (2025), also emphasised the lack of end-to-end security in institutional applications. Additionally, the nature of Universities complicates cybersecurity enforcement. This is because academic environments are often decentralised, with numerous departments with varying user roles and transient user populations. The open and collaborative culture in academia also conflicts more than imagined with security policies, thus resulting in inconsistent enforcement and vulnerability to breaches (Sasse *et al*., 2001). In Perotti *et al*. (2024), the authors emphasised that user-centred usability evaluation—particularly using tools like SUS and UEQ—can significantly enhance engagement and trust in e-learning platforms by aligning system design with user behaviour and experience.

3.0 Theoretical Framework

This study design, implements and evaluates a Data Protection Framework (DPF) for Information and Communication Technology (ICT) centers in universities. This was implemented at the Lagos State University of Science and Technology (LASUSTECH). This approach enables the validation of the approach. The resulting DPF bridges theoretical insight with the realities of institutional and offered a structured response to the complex cybersecurity challenges faced by universities and other higher institutions of learning, and ICT centers. The Framework Components of the DPF comprise four interdependent components as shown in Figure 1.

3.1 Access Control

The RBAC system ensures that users are only allowed to view the information necessary for their responsibilities. In computer systems security, role-based access control (RBAC), or role-based security, is an approach to restricting system access to authorised users. Role-based access control (RBAC) is a policy-neutral access control method defined in terms of roles and privileges. (Sandhu et al., 1996; Gilbert et al., 1995; Ferraiolo & Kuhn, 1992; Abreu et al., 2017). RBAC's components (role-permissions, user-role and role-role relationships) allow for easy user assignments.

3.1.1 Role-Based Access Control (RBAC)

Different job responsibilities will develop jobs inside the ICT directorate and the permission to undertake particular operations will be assigned to specific roles. Permissions are only granted to users through their roles. The management of individual user rights is simplified to the assignment of appropriate responsibilities to the user account, which facilitates simple actions like adding a user or altering a user's department. RBAC has three key operations: (1) Role assignment (A user can exercise a permission only if the user has been assigned a role or has selected a role). (2) Role authorisation (The active role of a user must be authorised to the user. With rule 1 above, this rule ensures that users can assume only roles for which they are authorised), and (3) Permission authorisation (A user can exercise a permission only if the permission is authorised for the user's active role). Rules 1 and 2. This rule ensures that users can exercise just the permissions they are approved for.

3.1.2 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a multi-step method to log into an account that needs users to enter more than simply a password. In addition to the password, users may be requested to input a code delivered to their email, answer a secret question or scan a fingerprint.

3.1.3 User Account Management

User account management is the process of managing user access by ensuring users have the appropriate level of access based on their role and responsibilities, user permissions by assigning right to systems, services, and applications. User authentication which allows users to log in and reset their passwords. User Role, which defines the different roles or groups of roles within a

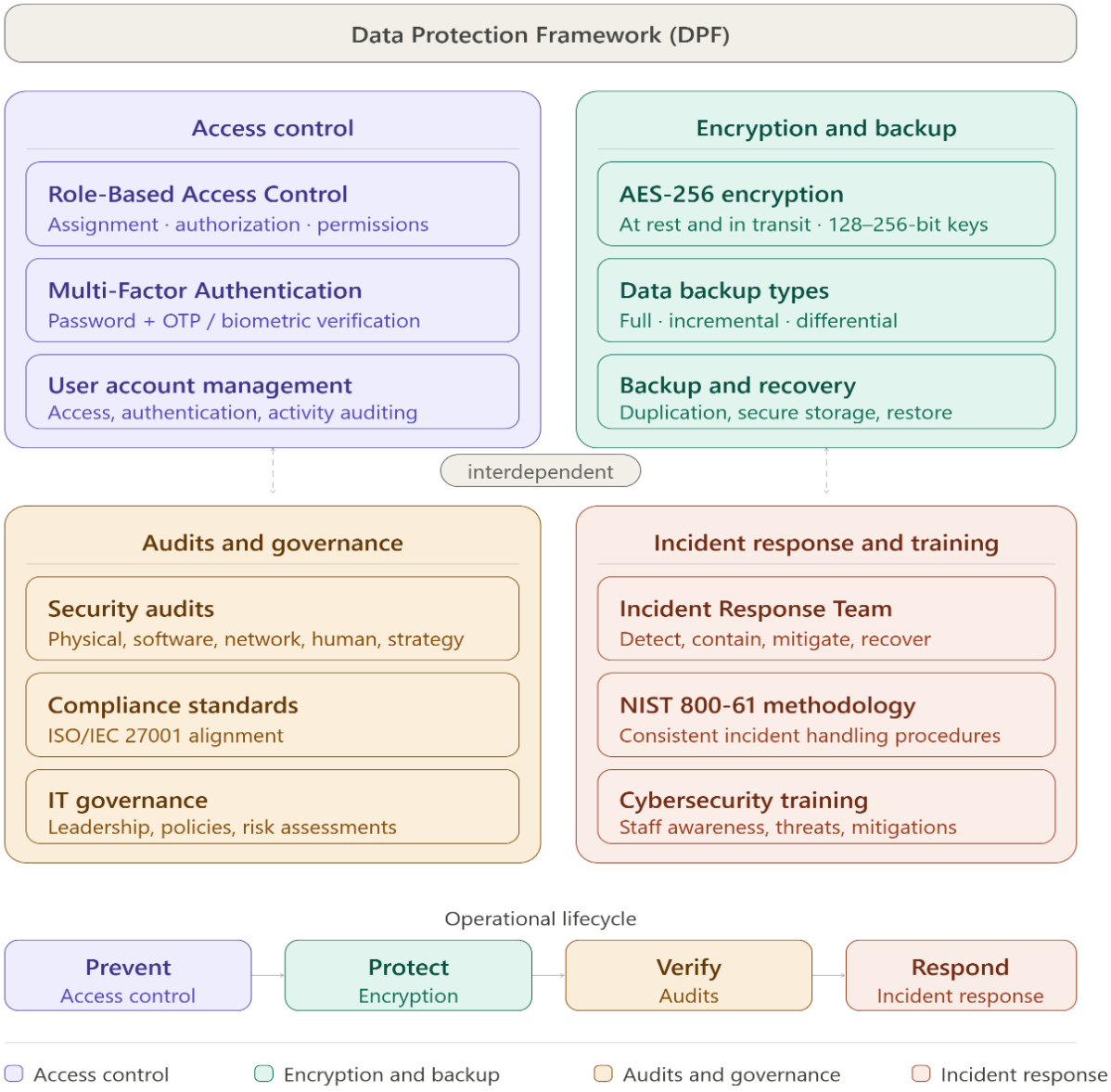

Figure 1: *Data Protection Framework designed for University ICT Centers*

software application, identity and access management which use technology and policies to manage digital identities and control their access to resources. User activity auditing monitors and record user account activities, Role-Based Access control grants user access based, User activity monitoring analyzes activity in an IT environment to identify user accounts that are accessing resources they should not be using. User account management software can automate the process of creating, modifying, and deactivating user accounts.

3.2 Encryption and Backup

Encryption is basic piece of information security that encodes human-readable information into an indecipherable arrangement by applying number crunching calculations. Only authorized users having a decryption key can fully restore the original data back to readable format. It protects data at rest, in transit across communication networks and in use in computing environments (i.e., on-premises or hosted infrastructure using cloud platforms). This has led to encryption being foundational in modern cyber and cloud security. The various encryption standards include Advanced Encryption Standard (AES), which is, in the most secure and widely used symmetric-key cryptographic algorithms. It is used for a lot of applications like VPNs, wireless communication systems, enterprise applications and operating environment. AES protects data in a series of cryptographic operations that substitute, permute and mix fixed-size blocks (128 bits) of the information using keys of 128, 192 or 256 bits. AES provides much higher levels of computational efficiency, a virtually limitless range of possible key and block lengths, and greater resistance to cryptanalytic attacks as compared with earlier standards such as the Data Encryption Standard (DES). Its very wide support on hardware and software has also led to widespread use. When used correctly AES is so secure that it cannot feasibly be decrypted without the right key. As a result, AES-256 is often used to protect sensitive

information at rest and in transit which ensures both data confidentiality and integrity even if transmissions go intercepted (Stallings, 2017). Except for the encryption, backup and recovery are important parts of information security and business continuity strategy. Data backup is simply making copies of data and storing it securely to restore in case of accidental deletion, system failure, cyberattack or any other loss of information. Generally, backup strategies can be divided into three principal categories. A full backup creates a complete replica of all the data related to a server, database, virtual machine, or another specified source of data. While this approach is comprehensive, it can be time- and storage-intensive, especially when dealing with massive amounts of information. An incremental backup saves only the changes since the last backup for less storage and faster performance. Incremental backups can however only be done after a full backup has been done first. Differential backups are a middle ground, and will include all information that has changed since the last full backup. Although differential backups use more disk space than its incremental counterpart, they typically make the recovery process easier and faster, since only the most recent full backup and most recent differential backup are required to restore your data. Encryption and backup strategies complement each other, providing a robust combination to protect your information assets while also ensuring business continuity when security incidents or operational disruptions may occur.

3.3 Regular Audits Compliance and Governance are conducted to detect vulnerabilities and meet the compliance of international standards such as ISO/IEC 27001 (ISO/IEC, 2013). A security audit is a thorough review of the institution's information systems. Generally, this review evaluates the processes of the ICT center against an audit checklist of industry best practices, set standards, and/or federal requirements. The security controls of an ICT center will be assessed in terms of an overall security audit for the following: (a) The physical components of your information system and the environment in which the information system is located. (b) Applications and software, including security patches that have already been installed by your systems administrators. (c) Network weaknesses, including public and private access and firewall settings (d) The human dimension including how employees collect, exchange and store highly sensitive information and (e) The business's overall security strategy including security rules, organization charts and risk assessments. Compliance and Governance is a framework for the leadership, organisational structures and business processes, standards and compliance to these standards, that ensures the organisation's IT supports and enables the achievement of its aims and objectives.

3.4 Incident response plan and training is crucial, there is therefore a need for an incident response capability to ensure that problems are detected quickly, loss and destruction are minimised, weaknesses exploited are mitigated and IT services are restored. Personal and company data are often compromised and it is vital to respond swiftly and efficiently when security breaches take place. The notion of computer security incident response has been widely adopted and applied. One of the benefits of having incident response capabilities is that it facilitates reacting to issues systematically (i.e., following a consistent incident handling methodology) so that the right measures are taken (NIST 800-61 Revision 2). An incident response framework defines processes for detecting, mitigating and recovering from security breaches. This means putting together an Incident Response Team (IRT). Staff also receive cybersecurity training on potential vulnerabilities and mitigations.

3.5 Ethical and legal considerations

All collected data were anonymised to protect institutional and individual privacy, and informed consent was obtained. Participation in interviews and assessments was voluntary, and the project adhered to the provisions of the Nigeria Data Protection Act (2023), NDPR, and institutional ethical guidelines. This alignment validates the framework's compliance with both international security standards and national regulatory requirements. It demonstrates that DPF is technically sound, legally grounded, and practically implementable, having met ISO/IEC 27001 benchmarks and passed regulatory checks in the Nigerian University context. In the following section, the architecture and operational implementation of the DPF are presented with the provision of detailed insights into its core modules and performance in a real-world university ICT environment.

4.0 Methodology

Towards the formulation of the framework, data inventory and classifications were carried out to identify the sensitivity of the different categories of data available at the ICT center. This was carried out to perform a comprehensive Risk Assessment to identify vulnerabilities and threats.

4.1 Vulnerability Assessment

E-mail/Social Networking, Unencrypted Devices, Cloud Storage Devices, Removable Media, Hardcopy and Improper Access Control are identified sources of vulnerabilities. Cybersecurity related vulnerabilities are eavesdropping attack, Data modification attack, IP address spoofing attack, Password based attack, Denial-of-Service (DoS) attack, Man-in-The-Middle (MiTM) attack, Compromised Key assault and sniffer attack. Table 1 shows the identified sources of Vulnerability and Table 2 shows the possible attacks.

Table 1: Sources of Vulnerability

S No.	Source	Cause of Vulnerability
1	Email/Social Networking	Instant messaging software and social media sites. intercepted email or chat could be captured and confidential information revealed.
2	Unencrypted Devices	A stolen official laptop containing confidential institutional data. If the data is not stored using an encryption algorithm, the thief can retrieve valuable confidential data.
3	Cloud Storage Devices	Sensitive data can be lost if access to the cloud is compromised due to weak security settings.
4	Removable Media	Unauthorized transfer of data to a USB drive or other removable storage can lead to data loss.
5	Hard Copy	Improper disposal of sensitive data. Documents containing confidential information not shredded when no longer required can be used malicious people to s and gain valuable information.
6	Improper Access Control	Passwords are the first line of defense. Stolen passwords or weak passwords which have been compromised can provide an attacker easy access to data.

Table 2: Types of Attacks

S No.	Category of Attack	Description
1.	Eavesdropping attack	This occur when a threat actor captures and listens to network traffic. This attack is also referred to as sniffing or snooping.
2.	Data modification attack	This is when a threat actor has captured enterprise traffic and has altered the data in the packets without the knowledge of the sender or receiver.
3.	IP address spoofing attack	A threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet
4.	Password-based attacks	Password-based attacks occur when a threat actor obtains the credentials for a valid user account. Threat actors then use that account to obtain lists of other users and network information. They could also change server and network configurations, and modify, reroute, or delete data.
5.	Denial-of-Service (DoS) attack	A DoS attack prevents normal use of a computer or network by valid users. After gaining access to a network, a DoS attack can crash applications or network services. A DoS attack can also flood a computer or the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.
6.	Man-in-The-Middle attack (MiTM)	A MiTM attack occurs when threat actors have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.
7.	Compromised key attack	A compromised key attack occurs when a threat actor obtains a secret key. This is referred to as a compromised key. A compromised key can be used to gain access to a secured communication without the sender or receiver being aware of the attack.
8.	Sniffer attack	A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted, and the threat actor does not have access to the key.

4.2 Data Protection Framework

The Data Protection Framework consists of the following components which are Access Control, Data Encryption and Backup, Audit and Compliance, and Incident Response and Training. These components are discussed in this section.

4.2.1 Access Control

To prevent unauthorised access to the resources at the ICT centre, different levels of access control were implemented in this work. Physical access control (Biometric-Based Access Control System) was implemented at the entrance of the server room, this is shown in Figure 2. The biometric access control was used to enhance the security systems of the Server room at the ICT building in order to add an extra layer of verification. It works by comparing the person's unique biometric characteristics, such as fingerprints, to a database of stored biometric templates about authorised users. If there is a match, the person is allowed in; otherwise, the person is denied access. It provides significant physical security benefits for protecting the Server room from intruders.

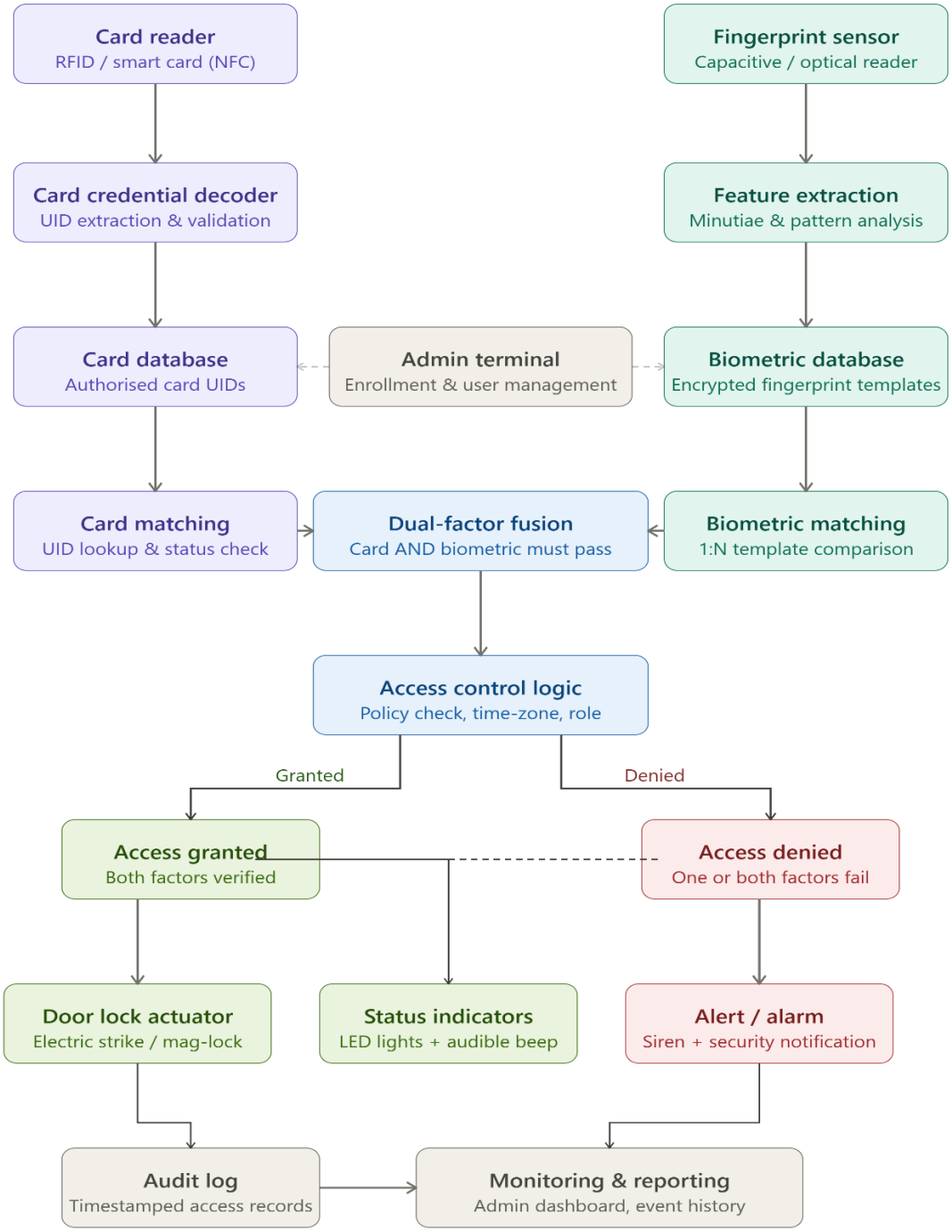

Figure 2: *Block diagram showing the functionality of the Biometric and Card-Based Access Control Implemented at the ICT Server Room*

4.2.2 Data Encryption and Backup

Sensitive data in transit and at rest are encrypted using AES-256 for storage and TLS 1.3 for web-based transmissions. Passwords and critical files undergo SHA-256 hashing. Key management protocols restrict access to decryption keys to authorised personnel through a centralised Key Management System (KMS).

LASUSTECH adopted a hybrid backup strategy involving daily incremental and weekly full backups. Backup data is encrypted and stored both on-premises and in the cloud. Periodic restoration tests validate recovery integrity. Recovery Time Objective (RTO) and RPO metrics were defined for key systems.

4.2.3 Auditing and Compliance

Auditing is semi-annual and covers physical, logical, and operational security practices. Monitoring tools were configured to track login patterns, data access logs, and system modifications. Logs are retained for 12 months in line with NDPA requirements. The framework is aligned with Nigeria's NDPA (2023), NDPR, and ISO/IEC 27001. A compliance office within the ICT Directorate was tasked with conducting periodic policy audits, maintaining documentation, and fulfilling regulatory reporting requirements. The governance structure includes an ICT compliance board and departmental ICT liaisons.

4.2.4 Incident Response mechanism

An Incident Response Team (IRT) was established with documented procedures for detecting, containing, and recovering from breaches. A multi-tier response plan was developed with severity-based categorisation: critical, high, medium, and low. Post-incident reviews are conducted to improve future responses.

4.2.5 Training and awareness

Cybersecurity awareness programmes were launched. It was meant to sensitize staff and students so they are aware of online threats and have the knowledge of best practices for safeguarding sensitive data. The training included phishing simulation drills, data handling protocols, and password hygiene. Training completion was monitored, and periodic refresher sessions were introduced.

5.0 Result and Discussion

The initial implementation of the DPF at LASUSTECH ICT Center has demonstrated significant improvements in LASUSTECH's security posture. Beginning with the physical access to the Server room. The privacy and security awareness created by the implementation of the DPF provides the needed consciousness in the ICT Directorate staff, students, University staff, visitors and vendors. This also increased staff and student participation in cybersecurity training programs. Furthermore, the work also highlights the adaptability of the framework to evolving security threats and its alignment with international best practices.

5.1 Framework impact assessment

The deployment of the DPF has been a resounding success. This was because it led to significant and reassuring improvements in our data security posture and institutional compliance, hence the following key outcomes:

- ***Access Control Enforcement:*** Post-deployment audits showed a 75% reduction in unauthorised access attempts to administrative systems.
- ***The adoption of*** MFA has significantly increased, now covering 91% of administrative and teaching staff accounts, providing a strong layer of protection.
- ***Incident Response Efficiency****:* The mean time to incident acknowledgement dropped from 24 hours to under 6 hours.
- ***Our periodic*** restoration tests have achieved a 100% success rate, with critical systems restored within an average of 3.5 hours, meeting the defined RTO and providing a high level of reliability.
- ***Training Participation:*** It was observed that awareness training completion increased from 42% to 86% across departments based on the experiences of realistic results using the DPF.

The rationale for applying these metrics stems from what they indicate (i.e., not only technical improvement but also behavioural alignment with security practices). These observed outcomes are summarised in Table 3, which provides a consolidated view of the key performance indicators (KPIs) following DPF deployment.

Table 3. *Summary of key performance indicators (KPIs) following DPF deployment at the case study site – LASUSTECH ICT Centre.*

Evaluation Metric	Pre-DPF Value	Post-DPF Value	Improvement (%) / Impact
Unauthorised Access Attempts	High (untracked)	Reduced by 75%	Significant reduction in breaches
MFA Adoption Rate	< 30%	91%	Major improvement in authentication coverage

Recovery Time Objective (RTO)	undefined (no RTO set)	4 hours (target met)	Recovery benchmark established and met consistently
Recovery Point Objective (RPO)	Undefined (no RPO set)	≤ 24 hours	Data loss contained within defined backup threshold
Incident Acknowledgement Time	24 hours average	Under 6 hours	75% faster incident response
Policy Visibility (staff feedback)	Low (anecdotal reports)	High (visible, documented)	Increased awareness and institutional clarity
Note: MFA (multi-factor authentication); RTO (Recovery Time Objective); RPO (Recovery Point Objective)			

As shown in the Table 3, the DPF led to substantial gains across all critical cybersecurity dimensions, underscoring its effectiveness as a modular, regulation-aligned framework suitable for Universities. It compares cybersecurity metrics at LASUSTECH before (*pre*) and after (*post*) DPF implementation, showing sharp reductions in unauthorised access and response time (i.e., incident acknowledgement time), alongside rises in MFA use and staff training. Recovery benchmarks were met as critical systems were restored within four hours (RTO), and data loss stayed (or avoided) within a 24-hour window (RPO). These outcomes demonstrate the framework's real-world value in Universities. Compared to studies (e.g., Krumay et al., 2020 & Armas and Taherdoost, 2025), the DPF adds value by integrating compliance and governance within a real University setting. Krumay's model emphasises macro-level accountability, while Armas and Taherdoost stress awareness—DPF bridges both. In comparison to conceptual models, the DPF - framework is field-tested. The field test results recorded improvements, which are tangible in terms of access control and relevant institutional engagement. Existing models often lack evidence of implementation. DPF fills this gap with measurable outcomes, including a 75% drop in access violations and successful recovery within the RTO benchmark. These measurable outcomes confirm its role as a practical, regulation-aligned solution for University cybersecurity challenges.

5.2 Perceptions from stakeholder feedback

A summary of post-implementation feedback from ICT and academic staff, and other stakeholders is presented as follows:

- ***Increased confidence****:* Staff reported stronger trust in institutional data handling.
- ***Usability versus control:*** Initial friction with MFA and role restrictions eased over time due to training.
- ***Policy visibility****: Staff and stakeholders acknowledged that* awareness increased as soon as clear and understandable guidelines were established.
- ***Support:*** There was also timely IT assistance and easy communication, which stakeholders agreed was critical to success.

5.3 Challenges Encountered

Despite the positive outcomes, the implementation was not without its operational and contextual challenges. As hurdles, the challenges were faced with corresponding efforts made to overcome them, and are acknowledged as follows:

- ***Resource Constraints****:* The team responsible for setting up the MFA and biometric control units experience unexpected delays. As a result, the initial budget was affected and needed reallocation.
- ***Change Resistance:*** A segment of staff resisted changes to access control and backup policies due to perceived disruptions to workflow.
- ***Technical Debt:*** This was in terms of timeliness due to the need to upgrade or replace the old systems that could not support encryption. The process of sorting these issues pushed back deadlines.

5.5 Limitations and Future Work

The scope of this study was limited to a single institution (LASUSTECH), which may affect generalisability. Legacy infrastructure also slowed implementation. Future work should test the DPF across universities with varying ICT maturity, extend it to mobile device governance, and explore AI-driven threat detection. Long-term audits and integration with ERP systems will further validate its scalability.

6.0 Conclusion and Recommendations

This study developed and presented a modular Data Privacy and Security Framework (DPF) tailored to the operational and regulatory landscape of higher education institutions, with deployment and evaluation at LASUSTECH. Anchored in design-science methodology, the DPF integrated technical controls, institutional governance, and legal compliance into a cohesive architecture.

The framework directly addressed key vulnerabilities—such as weak access controls, limited encryption, and the absence of incident response plans—identified during the baseline assessment. What followed after deployment was significant improvements. This was noted in access control enforcement, incident response readiness, data recovery capabilities, and user awareness. Stakeholder feedback corroborated all of these outcomes as they showed enhanced confidence in institutional practices, increased user engagement, higher training uptake, and the effectiveness of phased implementation.

Additionally, the case study institution made significant progress by applying the DPF and aligning so easily with all mandatory Data Protection Act (DPA) 2023 and ISO/IEC 27001 standards. The results prove that a flexible, regulation-focused approach can be strengthened to fortify cybersecurity and resilience, even in universities with limited resources. Due to its adaptability, the DPF can serve as a practical model for other higher education institutions—especially in developing regions working to meet compliance requirements while improving their capabilities.

6.1 Recommendations for policy and practice

Cybersecurity governance must be given the highest priority. It must be given a solid footing by the establishment of offices dedicated to enforce compliance. This approach would institutionalise it. There should also be cross-departmental ICT boards to ensure oversight. Institutions should invest intentionally in staff cybersecurity training, making it mandatory for all, with participation metrics to assess effectiveness. There should be incremental implementation of modular frameworks in resource-limited settings while prioritising RBAC, encryption, and backup modules. The continuous monitoring of key performance indicators must also be given high priority support. This should be accompanied by regular audits to sustain ongoing improvement. Lastly, there should be strong collaborations with stakeholders, regulators, and peer institutions to share best practices, pool resources, and influence policy development in line with evolving cybersecurity needs within higher education.

6.2 Directions for Future Research

Future work should explore the following: (i) Integration of AI-driven threat detection into institutional frameworks, (ii) Comparative evaluations of cybersecurity readiness across universities, especially resource constrained regions, (iii) Development of maturity models for assessing institutional data privacy posture, and (iv) Policy frameworks for mobile device and BYOD management in academic settings. This study contributes to existing literature, a tested and context-aware approach to cybersecurity in education. It reinforces the role of proactive governance and localised innovation in addressing global data protection challenges.

Acknowledgement

The authors express their sincere appreciation to the management of The Lagos State University of Science and Technology for the LASUSTECH Research Grant (LRG) 2023 which supported this research.

References

1. Abreu, V., Santin, A. O., Viegas, E. K., & Stihler, M. (2017). A multi-domain role activation model. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2017.7997247
2. Adams, A., & Blandford, A. (2003). Security and online learning: To protect or prohibit. In *Usability evaluation of online learning programs* (pp. 331–359).
3. Arina, A. (2022). Network security threats to higher education institutions. *Central and Eastern European eDem and eGov Days, 341*, 323–333. https://doi.org/10.24989/ocg.v341.24
4. Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. *Information, 16*(5), Article 336. https://doi.org/10.3390/info16050336
5. Babalola, O. (2022). Nigeria's data protection legal and institutional model: An overview. *International Data Privacy Law, 12*(1), 44–52. https://doi.org/10.1093/idpl/ipab024
6. Chaurasia, N., & Kumar, P. (2023). A comprehensive study on issues and challenges related to privacy and security in IoT. *e-Prime: Advances in Electrical Engineering, Electronics and Energy, 5*, Article 100158. https://doi.org/10.1016/j.prime.2023.100158
7. Ferraiolo, D. F., & Kuhn, D. R. (1992, October). Role-based access control. In *Proceedings of the*

15th National Computer Security Conference (pp. 554–563).

8. Gilbert, M. D., Lynch, N., & Ferraiolo, D. F. (1993). An examination of federal and commercial access control policy needs. In *Proceedings of the 16th National Computer Security Conference: Information Systems Security: User Choices* (p. 107). DIANE Publishing.

9. Krumay, B., Bernroider, E. W., & Walser, R. (2020). A framework to achieve cybersecurity accountability of critical infrastructure providers: A design science research approach. In *Conference of the Italian Chapter of the Association for Information Systems* (pp. 233–248). Springer. https://doi.org/10.1007/978-3-030-47411-9_16

10. Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). *Understanding cyber threats against universities, colleges, and schools* (arXiv Preprint No. arXiv:2307.07755). arXiv. https://doi.org/10.48550/arXiv.2307.07755

11. Manda, M. I. (2021). Leadership and trust as key pillars in smart governance for inclusive growth in the Fourth Industrial Revolution (4IR): Evidence from South Africa. In *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance* (pp. 308–315). https://doi.org/10.1145/3494193.3494304

12. Ngwenya, M., & Ngoepe, M. (2020). A framework for data security, privacy, and trust in consumer internet of things assemblages in South Africa. *Security and Privacy, 3*(5), e122. https://doi.org/10.1002/spy2.122

13. Nigeria Data Protection Act. (2023). *Nigeria Data Protection Act 2023 review*. KPMG Nigeria. https://kpmg.com/ng/en/home/insights/2023/08/nigeria-data-protection-act-2023-review.html

14. Perotti, L., Stamm, O., Dietrich, M., Buchem, I., & Müller-Werdan, U. (2024). The usability and user experience of an interactive e-learning platform to empower older adults when using electronic personal health records: An online intervention study. *Universal Access in the Information Society*, 1–16. https://doi.org/10.1007/s10209-024-01107-2

15. Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29*(2), 38–47. https://doi.org/10.1109/2.485845

16. Serb, A., Defta, C., Iacob, N. M., & Apetrei, M. C. (2013). Information security management in e-learning. *Knowledge Horizons, 5*(2), 55–59.

17. Siphambili, N. (2024). Exploring cybersecurity implications in higher education. In *European Conference on Cyber Warfare and Security* (Vol. 23, No. 1, pp. 526–531). https://doi.org/10.34190/eccws.23.1.2793

18. Song, K., Lee, S. M., & Nam, S. C. (2013). Combined biometrics for e-learning security. *Advanced Science and Technology Letters, 21*, 247–251. https://doi.org/10.14257/astl.2013.21.61

19. Sun, P., Wan, Y., Wu, Z., Fang, Z., & Li, Q. (2025). A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. *Computers & Security, 148*, Article 104097. https://doi.org/10.1016/j.cose.2024.104097

20. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), Article 39. https://doi.org/10.3390/fi13020039

21. Weippl, E., & Ebner, M. (2008). Security and privacy challenges in e-learning 2.0. In *Proceedings of the World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education* (Vol. 2008, No. 1, pp. 4001–4007).

22. Wong, J., Henderson, T., & Ball, K. (2022). Data protection for the common good: Developing a framework for a data protection-focused data common. *Data & Policy, 4*, e3. https://doi.org/10.1017/dap.2021.40