National Open University of Nigeria

Policy Title	NOUN Data Centre Policy
Policy No:	NQSA/POL/IGM/004
Owner:	National Open University of Nigeria (NOUN)
Approved By:	The University Senate
Manager/Driver:	Directorate of Management Information System (DMIS)
Date of Approval:	7th October, 2024
Date of Next Review:	October 2027

1.0 Introduction

Central to ensuring the integrity, security and use of data at the National Open University of Nigeria (NOUN) is data governance and Data Centre. The Data Centre is a repository of the university's data assets and a backbone that supports its e- learning, administrative, and research operations for informed decision making and institutional enhancement. Recognising its pivotal role, this policy provides a framework with clear guidelines,standards, and procedures to manage, protect, and optimise the institution's data resources.

2.0 Purpose

The policy aims to articulate the guidelines for ensuring that the university's digital resources are accessible, secure, and efficiently managed. This policy underscores NOUN's commitment to

upholding the highest standards of data integrity, security, and availability, ensuring that its stakeholders; ranging from students and faculty to researchers and administrators, can rely on the data centre's reliability and efficiency.

Scope

The scope of this policy covers the management, protection, utilisation, dissemination, and optimisation of university data with specific attention to:

3.1 Data archiving and retrieval
data integrity;

3.2 Data security;

3.3 Data availability; and

3.4 Data accessibility.

Definition

4.1 *Data: Information stored in an electronic format*

4.2 ***Data Centre*****:** A facility for computer systems and associated components, such as telecommunications and storage systems, backup power supplies, redundant data communications connections, environmental controls, and security devices.

Principles

5.1 NOUN is committed to ensuring safe storage and security of its data.

5.2 NOUN is committed to the management, upgrade, and maintenance of data centre infrastructure.

5.3 NOUN is committed to adhering to laid down standards and procedures for maintaining accurate and complete data.

5.4 NOUN is also committed to maintaining continuous access and ethical use of its data for informed decision making and institutional enhancement.

5.5 NOUN is committed to ensuring seamlessness and scalability of its data to meet institutional needs.

Policy Statements

6.1 Security and Privacy

6.1.1 Robust Protection: Advanced security protocols and technologies will be deployed to safeguard against unauthorized access, ensuring that data and systems are not compromised.

6.1.2 Continuous Monitoring: The Data Centre will be monitored round the clock to promptly detect and address any security threats or breaches, always ensuring data integrity and privacy.

6.1.3 User Authentication: Multi-factor authentication processes will be implemented to ensure only authorized personnel can access sensitive data and systems.

6.2 Availability

6.2.1 Reliable Uptime: By employing state-of-the-art infrastructure and redundancy measures, the Data Centre will aim for optimal uptime, ensuring that

systems and data are consistently available to authorized users.

6.2.2 Disaster Recovery: Plans and systems will be in place to swiftly restore operations in the event of any disruptions, ensuring minimizing downtime and data loss.

6.3 Scalability

6.3.1 Future-Proofing: The Data Centre's design will be forward-thinking, ensuring it can handle the ever-increasing data storage and processing demands of NOUN.

6.3.2 Flexible Infrastructure: Modular and scalable components will be integrated, allowing for easy expansions and upgrades as the university's needs evolve.

6.3.3 Change management: NOUN will employ effectiveand deliberate change management practices that will ensure availability, security and integrity.

6.4 Environmental Responsibility

6.4.1 Energy Efficiency: The Data Centre will utilize green technologies and practices to ensure optimize energy use, reducing the carbon footprint.

6.4.2 Sustainable Practices: From cooling systems to hardware disposal, the Data Centre will ensure that methods that are environmentally friendly are

prioritized, aligning with global sustainability standards and practices.

6.5 Access and Ethical Use

6.5.1 Usage of data shall be in accordance with the university's ethics policy

6.6 Data Governance and Management

6.6.1 NOUN shall have in place a central body responsible for the management of data governance and data centre as well as the policy.

6.6.2 NOUN shall have in place staff responsible for the daily operations, maintenance and management of the data centre

6.6.3 NOUN shall have in place staff responsible for ensuring data quality and compliance by users with policy and procedures, maintenance of data centre infrastructure and services.

Policy Implementation

7.1 Access and Security Protocols for the NOUN Data Centre

7.1.2 Physical Access

i. **Restricted Entry**: NOUN will ensure only personnel who have been pre-authorized, based on their roles and responsibilities, will be allowed physical access to the Data Centre. Unauthorized entry attempts will trigger alerts.

ii. **Entry and Exit Logs**: Detailed logs capturing the time, date, and identity of every individual accessing the Data Centre will be maintained. This ensures traceability and accountability for all physical interactions within the facility.

7.1.2 Digital Access

i. Robust Authentication: To safeguard against unauthorized digital access, rigorous authentication protocols, including multi-factor authentication and encrypted credentials, will be enforced.

ii. User Privilege Management: Users will be granted privileges strictly based on their roles, ensuring they can only access data and systems relevant to their responsibilities.

7.1.3 Continuous Monitoring

i. Surveillance: State-of-the-art surveillance cameras will be strategically positioned to monitor the Data Centre's premises continuously, capturing any unusual activity.

ii. Intrusion Detection: Sophisticated intrusion detection systems will be in place to detect any unauthorized or malicious activities, both digital and physical, triggering immediate alerts to security personnel.

iii. NOUN will engage in intrusion and detection research to enhance the security of the institutions network.

7.1.4 Firewall and Network Security

i. Proactive Protection: The Data Centre will employ advanced firewalls that do not ensure only threats are blocked but also analyse traffic patterns to detect potential anomalies.

ii. Regular Updates: Network security tools will be kept up-to-date to defend against the latest cyber threats, ensuring the Data Centre remains a fortress against evolving digital challenges.

7.2 Data Centre Operations and Comprehensive Management

7.2.1 Backup and Disaster Recovery:

i. Regular Backups: The Data Centre will conduct frequent data backups to safeguard against potential data loss. This includes incremental backups forreal-time data and full backups at scheduledintervals.

ii. Disaster Recovery Protocols: Comprehensive disaster recovery plans will be developed, outlining procedures to restore data and system functionality in the event of unforeseen calamities or system failures.

7.2.2 Routine Maintenance and Updates

i. Scheduled Maintenance: To ensure the consistent and optimal performance of all infrastructure, regular maintenance sessions will be scheduled outside of peak usage times to minimize disruptions.

ii. Software and Firmware Updates: All systems within the Data Centre will be periodically updated to incorporate the latest security patches, functionality enhancements, and other crucial updates.

7.2.3 Environmental and Safety Controls

i. Climate Management: The Data Centre will maintain optimal environmental conditions through advanced temperature and humidity control systems, ensuring the longevity and efficiency of hardware components.

ii. Fire Safety: The state-of-the-art fire detection and suppression systems will be installed, designed to quickly detect, and mitigate fire risks while minimizing potential damage to equipment and data.

7.2.4 Uninterrupted Power Management

i. Redundant Power Supplies: To ensure continuous operations, the Data Centre will have multiple power sources, instantly switching to backups in case of primary power failures.

ii. UPS and Generators: An Uninterruptible Power Supply (UPS) will provide immediate backup power during short-term power interruptions, while backup generators will be on standby for longer outages, ensuring continuous power supply and preventing data loss or system shutdowns.

7.2.5 Compliance with Legal Requirements

NOUN will comply with Nigeria Data Protection laws in accordance with the provisions of the laws.

7.3 Scalability and Continuous Infrastructure Enhancement

7.3.1 Periodic Infrastructure Assessment

i. Capacity Analysis: Regular evaluations will monitor the current usage of the Data Centre's storage, computing, and network capacities.

ii. Performance Benchmarking: Performance metrics will be benchmarked against industry standards and expected outcomes to ensure optimal efficiency.

7.3.2 Strategic Upgrades

i. Technology Refresh: As technological advancements emerge, the Data Centre will integrate the state-of-the-art hardware and software solutions to stay at the forefront of data processing and storage capabilities.

ii. Review-Driven Enhancements: Upgrades will be strategically implemented, based on the insights from infrastructure assessments, ensuring that the Data Centre evolves in alignment with NOUN's growing requirements.

7.3.3 Future-Ready Expansion

i. Physical Space Augmentation: As data and processing demands increase, provisions will be made for the potential physical expansion and enhancement of the Data Centre facility.

ii. Modular Design: Embracing a modular design approach ensures that the Data Centre can scale its infrastructure components efficiently without major overhauls, offering flexibility for future growth.

7.4 Environmental Responsibility

7.4.1 Commitment to Energy Efficiency

i. **Optimized Hardware**: The Data Centre will deploy state-of-the-art, energy-efficient servers, storage systems, and network devices to minimize power consumption.

ii. **Advanced Cooling**: Innovative cooling solutions, such as liquid cooling and hot/cold aisle containment, will be used to maintain optimal temperatures, thereby reducing the energy footprint.

iii. **Power Usage Effectiveness (PUE)**: Regular monitoring of the Data Centre's PUE, a standard metric for the efficiency of data centre power usage, will ensure that energy consumption remains within the desired thresholds.

7.4.2 Embracing Sustainable Practices

i. **Green Technologies**: The Data Centre will explore and integrate renewable energy sources, such as solar or wind power, to reduce reliance on non-renewable energy.

ii. **Carbon Footprint Reduction**: Efforts will be made to continuously evaluate and minimize the Data Centre's carbon emissions, aligning with global sustainability goals.

iii. **Energy Management Systems**: Automatedsystems will monitor and control energy consumption, ensuring that resources are used judiciously, and wastage is minimized.

7.4.3 Waste Management and Equipment Lifecycle

i. **Responsible Disposal**: Outdated or non-functional equipment will be disposed of in accordance with environmental guidelines, ensuring minimal environmental impact.

ii. **Eco-Friendly Procurement**: When procuring new equipment or materials, preference will be given to products with eco-friendly certifications or those that adhere to sustainable manufacturing practices.

7.4.4 Data Archiving and Retrieval

Archiving

i. A d**ata Retention Schedule** shall be established based on data type, usage, and regulatory requirements.

ii. **Archival Storage**: Secure, long-term storage solutions for archived data shall be utilised to ensuring data integrity and accessibility.

iii. **Regular Backups**: Regular backups of critical data shall be undertaken to prevent data loss and ensure availability in case of system failures.

Retrieval

iv. **Access Control**: Implement strict access controls to ensure only authorized personnel can retrieve archived data.

v. **Efficient Retrieval Systems**: Develop and maintain efficient systems for locating and retrieving archived data promptly.

vi. **Audit Trails**: Maintain detailed logs of data retrieval activities to ensure accountability and traceability.

8.0 Sanctions on Violating this Policy

Any staff that violates this policy will face disciplinary actions in accordance with the university's conditions of service.

Policy Alignment

This policy aligns with:

9.1 NOUN Blueprint
9.2 Getting to know your university.
9.3 NOUN Strategic Plans
9.4 Digital Transformation Strategy
9.5 National Data
9.6 NOUN's Conditions of Service (2016)
9.7 NOUN's Research Ethics Policy.

10.0 Team of Developers

1. Professor Godwin Akper
2. Dr. Adewale Adesina
3. Dr. Greg Onwodi
4. Mr. Adeyinka M. Adeboyejo
5. Mr. Sule Onuh
6. Mr. Olatunji Folami