UNIVERSITY OF ILORIN

COMPUTER SERVICES AND INFORMATION TECHNOLOGY (COMSIT) DIRECTORATE

2025- 2035

OPERATIONAL BLUEPRINT

JUNE, 2026

Table of Contents

Executive Summary

As the Director of Computer Services and Technology (COMSIT) at the University of Ilorin, it is my privilege to present this operational blueprint for the Directorate. This document outlines the Directorate's strategic vision and operational framework, which is designed to enhance the Information and Communication Technology (ICT) landscape of the university while supporting the mission of achieving quality ICT service delivery.

The Directorate comprises 12 specialized units, each with distinct but interrelated functions that collectively contribute to the university's digital ecosystem:

1. Administration and Operations Unit: supports the overall administration of the Directorate, ensuring that the day-to-day operations are efficiently delivered in alignment with the university goals.

2. Cybersecurity and Multimedia Unit: sees to the protection of the university's digital assets against cyber threats while promoting safe and responsible use of ICT.

3. Digital Innovation and ICT Ideation Unit: Drives innovation in technology usage across the university, fostering a culture of digital creativity and problem-solving.

4. Electronic Learning and Assessment Unit: Dedicated to advancing our e-learning capabilities, this unit ensures robust online educational platforms and assessment tools are available and effective.

5. IT Officers Coordinating Unit: oversees the activities of all IT personnel posted across the campus, ensuring effective collaboration and support for all technology-related initiatives.

6. Mail Services and Help Desk Unit: Facilitates effective communication and provides technical support to the university community.

7. Network Operations Unit: manages and maintains the university's network infrastructure, ensuring reliable connectivity for all users.

8. Portal Unit: responsible for maintaining and enhancing the university's digital interface, ensuring seamless access to information and services for students, faculty, and staff.

9. Software and Applications Development Unit: focuses on the development, implementation, and management of software applications that cater to the diverse needs of the university community.

10. Software Hardware Installation, Repairs, and Maintenance Unit: ensures that all hardware and software systems are operational, up-to-date, and efficiently maintained.

11. Training Unit: provides training programs for staff and students to enhance their digital skills and proficiency in using university systems and tools.

12. Web Services/Help-desk Unit: manages the university's web presence, ensuring that our online resources are user-friendly, informative, and up-to-date.

This operational blueprint serves as a road map for our initiatives over the next 10 years. It emphasizes collaboration, innovation, and continuous improvement to meet the evolving needs of our university community. With the support of all stakeholders, we are committed to fostering an environment where technology enhances education, research, and administration.

Together, we can leverage ICT to transform the University of Ilorin into a leading institution in the digital age thus achieving the vision 1:10:500 of the current administration.

Prof. Rasheed Gbenga Jimoh, FNCS
Director, Directorate of Computer Services and Technology (COMSIT), University of Ilorin

Foreword

It is with great enthusiasm that I introduce the operational blueprint for the Directorate of Computer Services and Technology (COMSIT) at the University of Ilorin. In an era driven by rapid technological advancements, our commitment to integrating innovative solutions into our educational landscape has never been more crucial.

This blueprint, crafted with input from our dedicated professionals, outlines a comprehensive strategy that aligns with our university's vision of excellence in education, research, and community service. The 12 sub-units within the Directorate have been carefully designed to address the multifaceted challenges and opportunities presented by the digital landscape.

As we move forward, our focus will remain on ensuring that technology serves as a catalyst for enhancing the educational experience of our students and the operational efficiency of our faculty and non-teaching staff. By fostering a culture of collaboration and continuous learning, we aim to position the University of Ilorin at the forefront of educational technology.

I encourage all members of our university community to engage with this blueprint and contribute to our collective efforts in achieving our goals. Together, we will harness the power of technology to realize our aspirations and drive the University of Ilorin towards greater heights.

Thank you for your commitment to excellence and innovations at our better by far University.

Prof. Wahab Olasupo EGBEWOLE, SAN
Vice Chancellor, University of Ilorin

Brief Overview of the Directorate

The Directorate of Computer Services and Information Technology was formed through the merger of three existing IT departments at the University: the Computer Centre, the Management Information System Unit (MIS), and the Unilorin Nigeria Universities Network Office (Unilorin NUNet).

1. **Computer Centre**: Headed by Mr. T. I. Aiyelabegan as Director.
2. **Management Information System Unit (MIS)**: Led by Mrs. O.V. Mejabi as Acting Head.
3. **Unilorin NUNet**: Directed by Dr. T.S. Ibiyemi of Electrical Engineering, who served as Head and Chairman.

Each unit originally reported to separate boards. However, these boards were dissolved following the implementation of a new ICT Policy and Strategic Plan in 2001/2002 by the University through the Academic Planning Unit.
In 2002, the office of the Director of Academic Planning Unit convened the first meeting of COMSIT as a merger, with Mr. T. I. Aiyelabegan as the Director of the Directorate, Mrs. J. Olorunfemi as Head of the Computer Centre, Mrs. O.V. Mejabi as Head of MIS, and Engr. Sogo Popoola as Head of the Unilorin NUNet office. Post-merger, these units evolved to meet the IT demands of the University community.
To establish a robust IT team and foster an ICT-driven academic environment at the University of Ilorin, all IT staff from academic departments, laboratories, centres, and units were integrated into COMSIT in alignment with the ICT Policy and Strategic Plan 2003-2008.

- The **Computer Centre** continued its training programs and technical support for academic laboratories.
- The **MIS Unit** developed applications and deployed a portal system for students and staff in 2007/2008.
- The **NUNet Office**, known for supporting email services through dial-up technologies, registered a fully qualified domain name for the University in 2003, leading to the launch of web services and campus-wide networking.

The merger achieved remarkable success. The portal development, the first of its kind in any Nigerian institution, brought Unilorin to the limelight. The University was ranked the best in the country three times and placed as runners-up in subsequent years by Webometrics.info and 4icu.org (now Unirank) between 2008 and 2014.
Subsequently, a **Helpdesk Unit** was established to provide technical support to staff and students on the use of the portal and to act as a computer emergency response or computer security incident response team (CERT/CSIRT).

S/N	Directors Up to Date	Duration
1	Prof. Rasheed Gbenga Jimoh	1st August 2023 till date
2	Prof. Dupe Ademola-Popoola	21st December, 2020- 31st July, 2023
3	Prof O.V. Mejabi	1st August, 2020 to 20th December, 2020
4	Prof. Yinusa Adediran	1st August, 2019 to 31st July, 2020
5	Prof. Mudasiru Olalere Yusuf	1st August, 2017 to 31st July, 2019
6	Prof. Musa I. Ahmed	1st August, 2014 to 31st July, 2017
7	Prof. Isaac Abiodun Adimula	1st August, 2011 to 31st July, 2014
8	Mr. Taiye Issa Aiyelabegan	1st August, 1997 to 31st July, 2012

Overview of the Operational Blueprint

The operational blueprint for the Directorate of Computer Services and Technology at the University of Ilorin serves as a strategic framework designed to enhance our technological capabilities and align them with the university's overarching mission of delivering high-quality education, fostering research, and serving the community. In an era where technology is integral to all aspects of academia, the Directorate stands committed to leveraging these advancements to create a dynamic and innovative educational environment.

This blueprint encompasses 12 specialized units, each tailored to address specific technological needs and challenges within the university. By fostering collaboration among these units, we aim to provide integrated solutions that enhance the experiences of students, faculty, and administrative staff alike.

Key Objectives

1. P**ortal Unit:** This unit is responsible for the continuous improvement and maintenance of the university's digital portal, ensuring that it serves as a comprehensive gateway for accessing academic resources, administrative services, and campus information. Key objectives include enhancing user experience through intuitive design, improving accessibility for all users, and integrating various university functions such as course registration, schedules, and announcements.

2. **Software and Applications Development Unit :** Focused on developing and managing bespoke software applications, this unit aims to address the unique needs of our university community. Objectives include streamlining administrative processes, enhancing academic management systems, and implementing user-friendly applications that facilitate communication and collaboration among students and faculty.

3. Electronic Learning and Assessment Unit: This unit is dedicated to advancing the university's e-learning capabilities. Key objectives include developing robust online learning platforms, creating engaging digital content, and ensuring reliable assessment tools that support both formative and summative evaluations, ultimately enhancing the overall online learning experience.

4. Web Services/Help-desk Unit : Responsible for managing the university's web presence, the Web Services unit aims to create a user-friendly, informative, and visually appealing website. Objectives include ensuring that all web content is current, optimizing site performance for speed and accessibility, and integrating interactive features that enhance user engagement.

5. Digital Innovation and ICT Ideation Unit : This unit drives innovation within the university by fostering a culture of creative problem-solving and digital experimentation. Key objectives include organizing hackathons and innovation challenges, collaborating with academic departments to integrate technology into curricula, and exploring emerging technologies that can enhance the educational experience.

6. IT Officers Coordinating Unit : This unit oversees the coordination of IT personnel across the university, ensuring effective collaboration and support for all technology-related initiatives. Objectives include standardizing IT practices, providing ongoing professional development for IT staff, and facilitating communication between units to address technological needs efficiently.

7. Training Unit : Focused on enhancing the digital skills of both staff and students, this unit provides comprehensive training programs on various technology platforms and tools. Key objectives include assessing training needs, developing tailored training modules, and ensuring that all users are equipped to utilize technology effectively to support their academic and administrative functions.

8. Cybersecurity and Multimedia Unit : This unit plays a crucial role in safeguarding the university's digital assets against potential cyber threats. Objectives include implementing robust security protocols, conducting regular security audits, and providing training on safe online practices for all members of the university community.

9. Software and Hardware Installation, Repairs, and Maintenance Unit : Responsible for ensuring that all IT equipment and software are functioning optimally, this unit's objectives include establishing a routine maintenance schedule, providing timely repairs, and ensuring that all hardware and software installations meet the university’s standards and requirements.

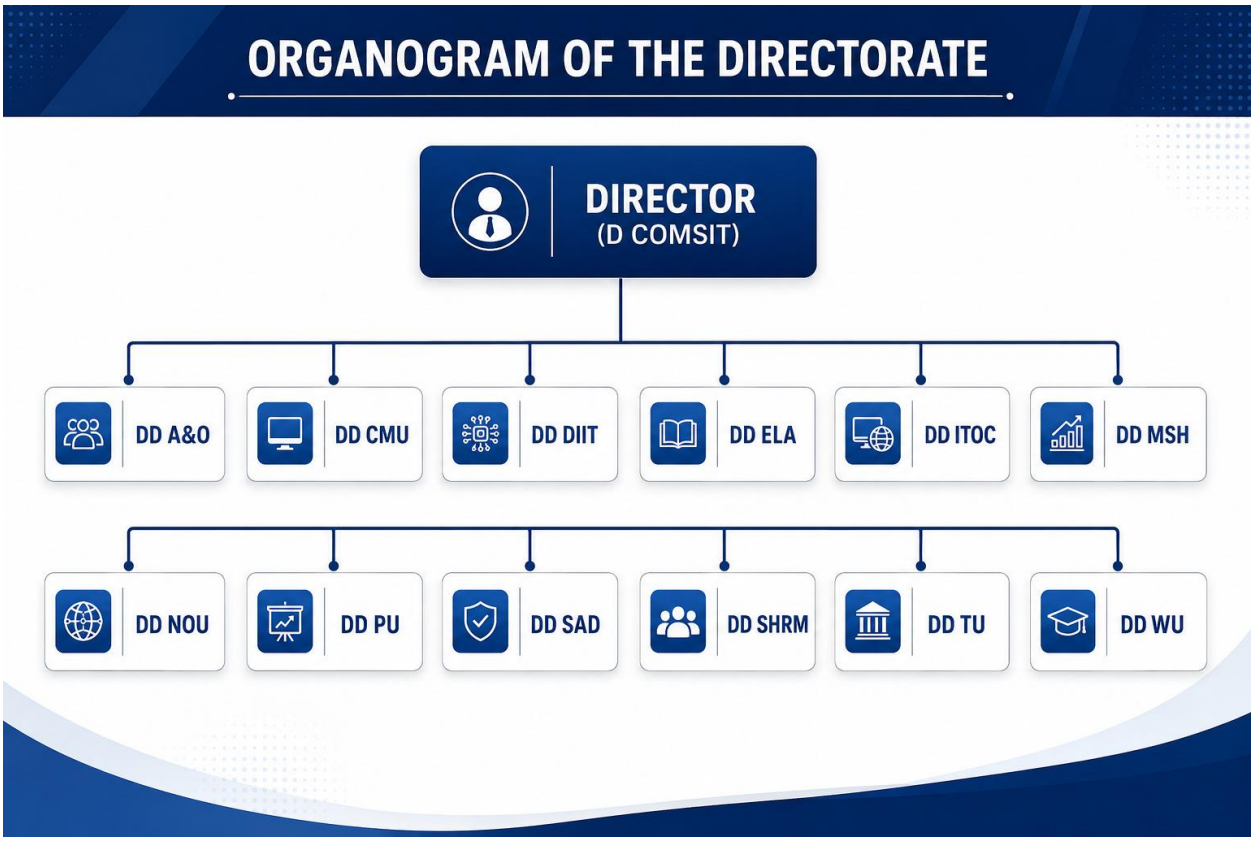
10. Mail Services and Help Desk Unit : This unit facilitates effective communication and provides technical support to the university community. Key objectives include streamlining mail services, establishing a responsive help desk system, and ensuring that all users receive prompt assistance for their technical inquiries.

11. Network Operations Unit : Tasked with managing and maintaining the university's network infrastructure, this unit aims to ensure reliable connectivity for all users. Objectives include monitoring network performance, implementing necessary upgrades, and ensuring secure access to university resources across campus.

12. Administrations and Operations Unit : This unit supports the overall administration of the Directorate, focusing on operational efficiency and alignment with university goals. Key objectives include optimizing resource allocation, enhancing communication within the Directorate, and ensuring compliance with university policies and standards.

This operational blueprint represents a forward-thinking approach to technology management, providing a road map for the Directorate to evolve in response to emerging trends and the needs of our university community. By focusing on these key objectives, the Directorate of Computer Services and Technology aims to lead the digital transformation at the University of Ilorin, ultimately enriching the educational experience and fostering a culture of innovation and excellence.

Organogram of the Directorate



Acknowledgments

The successful development of the operational blueprint for the Directorate of Computer Services and Technology at the University of Ilorin is the result of the collective efforts, dedication, and expertise of numerous individuals and teams across our university community.

We would like to extend our sincere gratitude to everyone who contributed to this important initiative.

First and foremost, we wish to acknowledge the leadership and vision of the Vice Chancellor, who has been a steadfast advocate for the integration of ICT in teaching research and university and administration. Your support has been instrumental in guiding this project and aligning it with the university's strategic goals.

We express our appreciation to all staff members of the Directorate of Computer Services and Technology, including the heads and team members of the 12 units. Your insights, expertise, and unwavering commitment to excellence have shaped the framework of this blueprint. Each unit has played a vital role in detailing its objectives and initiatives, ensuring that we address the diverse needs of our university community effectively.

We are confident that, with the collaborative spirit and commitment demonstrated by all involved, this operational blueprint will serve as a vital guide in our journey toward technological excellence at the University of Ilorin.

Thank you for your dedication and support in making this vision a reality.

List of Abbreviations and Acronyms

Abbreviation	Meaning
ICT	Information and Communications Technology

IoT	Internet of Things
AI	Artificial Intelligence
MIS	Management Information System
NUNET	Nigeria University Network
COMSIT	
AOU	Administration and Operations Unit
NOC	Network Operating System
Computer	Management and Information System
CSMU	Cyber Security and Multimedia Unit
DIICTIU	Digital Innovation and ICT Ideation Unit
RPA	Robotic Process Automation
VA/VR	Virtual Augmented Automatin
KPI	Key Performance Indications
NOU	Network Operations Unit
HTSU	Helpdesk and Technical Support Unit
TU	Training Unit
SHIRM	Software and Hardware Installations, Repair and Maintenance
SADU	Software and Application Development Unit
ELA	Electronic Learning and Assessment Unit
ITCU	IT Officer Coordinating Unit
WSU	Web Services Unit
SOP	Standard Operating Procedure
S	Strength W Waekness O Opportunity T Treat
REST	Representational Structure
S	Simple O Object A Access P Protocol
SSL	Secure Socket Layer
TLS	Transport Layers Security
LDAP	"Lightweight Directory Access Protocol".

Introduction

The rapid advancement of technology has transformed the landscape of higher education, making it imperative for institutions to adapt and innovate continually. The University of Ilorin recognizes the critical role that technology plays in enhancing educational quality, streamlining administrative processes, and fostering research and collaboration. In response to these challenges and opportunities, the Directorate of Computer Services and Technology has developed this operational blueprint. This document serves as a strategic framework that outlines our objectives, priorities, and initiatives designed to optimize the use of technology across the university.

The operational blueprint is built upon the foundation of 12 specialized sub-units, each contributing to the overall mission of the Directorate. By integrating the efforts of these units, we aim to create a cohesive and effective technological ecosystem that supports the diverse needs of our university community. This blueprint not only reflects our commitment to excellence but also positions the University of Ilorin as a leader in the digital transformation of a 21st century higher institution.

Scope of the Blueprint

The scope of this operational blueprint is to provide a comprehensive framework for the Directorate of Computer Services and Information Technology, guiding our strategic initiatives and operational practices over the coming years. It aims to:

1. Define Strategic Objectives : Establish clear goals for each of the 12 sub-units, ensuring that all technology-related initiatives are aligned with the university's mission and vision.

2. Enhance Collaboration : Foster collaboration among various units within the Directorate and across the university, promoting a unified approach to technology implementation and innovation.

3. Improve Service Delivery : Streamline processes and enhance the quality of services provided to students, faculty, and administrative staff, ensuring that technology serves as a facilitator of success.

4. Encourage Innovation : Create an environment where new ideas and technological advancements are embraced and explored, driving continuous improvement and adaptation to emerging trends.

The scope of this blueprint encompasses all aspects of ICT management within the Directorate, including software and applications development, e-learning initiatives, cybersecurity measures, IT support, and network operations, among others. It serves as a guiding document for the

allocation of resources, prioritization of projects, and evaluation of outcomes, ultimately contributing to the university's long-term goals.

Importance and relevance of the project

The operational blueprint for the Directorate of Computer Services and Technology is of paramount importance for several reasons:

1. Response to Evolving Educational Needs : As the educational landscape continues to evolve, the university must be proactive in adopting technologies that enhance learning experiences, facilitate remote education, and meet the diverse needs of students and faculty.

2. Enhancement of Operational Efficiency : By establishing clear objectives and streamlined processes, the blueprint will enable the Directorate to improve operational efficiency and service delivery, reducing downtime and enhancing user satisfaction.

3. Support for Research and Innovation : The blueprint emphasizes the importance of fostering a culture of innovation and digital ideation, which is essential for advancing research initiatives and ensuring that the university remains competitive in a global academic environment.

4. Strengthening Cybersecurity Measures : In an age of increasing cyber threats, the blueprint highlights the necessity of robust cybersecurity protocols to protect sensitive information and maintain the integrity of university systems.

5. Alignment with Institutional Goals : The operational blueprint ensures that all technology initiatives are aligned with the broader goals of the university, fostering collaboration and synergy among departments and enhancing the overall educational experience.

Operational Blueprints for Units and Administration and Operations Unit

COMPUTER SERVICES AND INFORMATION TECHNOLOGY (COMSIT) DIRECTORATE

A. OPERATIONAL BRIEF

The unit shall coordinate all activities of other units of the Directorate in addition to handling all administrative matters bordering on the day-to-day running of the Directorate. The Head of the Unit shall equally put all administrative staff of the Directorate into their optimal performance.

B. INTRODUCTION

Deputy Director, Administration and Operations, provides strategic direction, oversight, and support to the units within COMSIT Directorate based on director's instruction. The unit aims to streamline operations, enhance service delivery, and foster collaboration among these units to achieve the Directorate's objectives, mandate and meet the institution's technological needs.

The role of the Deputy Director, Administration and Operations, within the ICT Directorate is pivotal in driving operational excellence, fostering innovation, and ensuring seamless collaboration among the diverse array of units under their purview.

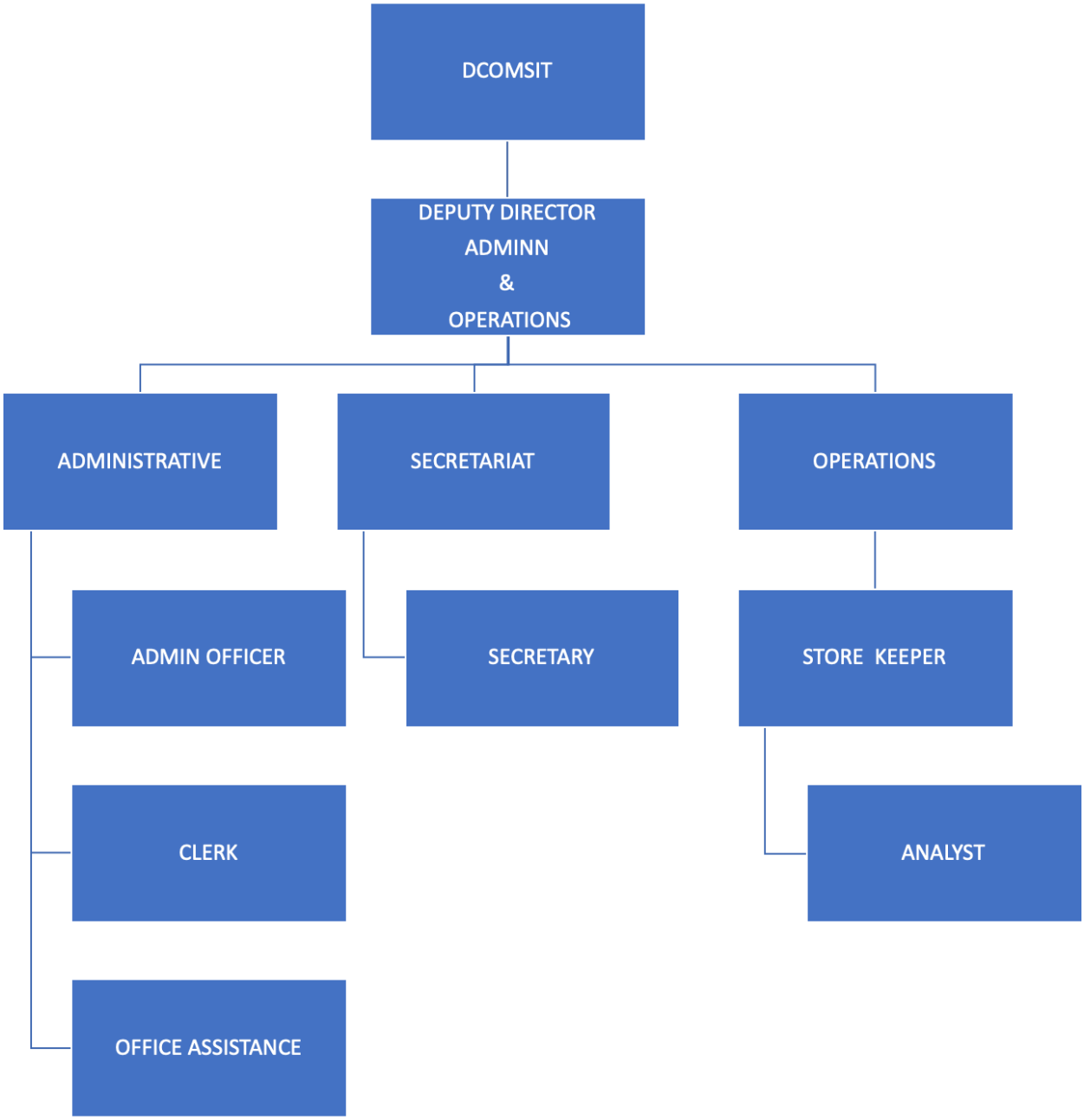
C. MISSION STATEMENT

The unit is established to see to the smoothness of day-to-day running of the COMSIT Directorate.

D. STAFFING

Head of Unit(1): Superintend on behalf of the DCOMSIT to provide strategic leadership and general oversight Secretary(1):Coordinates and Support the unit head and oversees administrative tasks within the Directorate Administrative Officer(1):Assists the Secretary to handle day-to-day administrative duties. Clerical Officer(1):Assist the secretary of the unit in mail distribution, documentation and information dissemination. Store keeper(1):Keeping inventory of all ICT assets, gadgets and in the unit. Systems Analyst (1):Assisting the Head of the unit in analysing the activities of all other units in the directorate

E. UNIT ORGANOGRAM



F. SWOT ANALYSIS

Strengths:

On strict directive of the Director of COMSIT, the A & O has the following:

1. Centralized oversight and coordination of critical administrative and operational services, including resource allocation, management and decommissioning.
2. Ability to streamline and standardize processes across all units.
3. Access to a diverse pool of skilled professionals within the units.
4. Potential for synergies and collaborative initiatives among the units.

Weaknesses:

1. Potential communication barriers or silo operations among the units.
2. Difficulties in balancing competing priorities and demands from different units of COMSIT Directorate.
3. Potential resistance to change or new policies from unit staff.

Opportunities:

On strict directive of the Director of COMSIT, the A & O has the following:

1. Leverage digital transformation initiatives to enhance service delivery and operational efficiency.
2. Explore automation and process optimization opportunities across units.
3. Foster partnerships with external organizations for professional development or resource sharing.

Threats:

1. Rapid technological advancements outpacing the skills and resources of the units.
2. Budgetary constraints limiting investment in infrastructure, tools, and staff development.
3. Cybersecurity threats and data breaches posing risks to the institution's digital assets.
4. Staff attrition and difficulties in attracting and retaining top talent.
5. Changing regulatory or compliance requirements impacting unit operations.

G. KEY PERFORMANCE INDICATORS (KPIs)

Deputy Director, Administration and Operations

1. Strategic Plan Implementation Rate: Percentage of strategic initiatives successfully implemented within the specified time frame.
2. Policy Compliance Rate: Adherence to University policies and COMSIT objectives.

Head of Unit

1. Operational Efficiency: Reduction in operational bottlenecks and time taken to complete unit tasks.
2. Staff Performance: Average performance rating of unit staff.

Secretary

1. Schedule Management: Number of scheduling conflicts resolved and meetings arranged per month.
2. Administrative Task Completion Rate: Percentage of administrative tasks completed on time.

Administrative Officer

1. Task Efficiency: Time taken to complete routine administrative tasks.
2. Project Success Rate: Percentage of specific projects completed successfully and on time.

Clerical Officer

1. Document Accuracy: Percentage of documents filed accurately and timely.
2. Mail Handling Efficiency: Average time taken to manage mail and distribute documents.

Storekeeper

1. Inventory Accuracy: Accuracy of inventory records compared to physical inventory counts.
2. Procurement Efficiency: Time taken to procure supplies and equipment, and compliance with University procurement policies.

Systems Analyst

1. Data Analysis Quality: Quality and accuracy of data-driven insights provided.
2. Efficiency Improvement Rate: Percentage increase in efficiency of other COMSIT units based on recommendations.

H. STANDARD OPERATING PROCEDURES

1. PURPOSE: This SOP defines the roles, responsibilities, and operational procedures for the Administration and Operations unit within the COMSIT Directorate. The aim is to ensure efficient and effective support of all COMSIT units and the University of Ilorin.
II. SCOPE: This SOP applies to all staff members of the Administration and Operations unit, including the Head of Unit, Secretary, Administrative Officer, Clerical Officer, Storekeeper, and Systems Analyst.

III. RESPONSIBILITIES & REPORTING STRUCTURE:

1. Deputy Director, Administration and Operations: Overall responsibility for the unit's strategic direction, performance, and alignment with University ICT policy and COMSIT objectives. Reports directly to the Director of COMSIT.
2. Head of Unit: Day-to-day management of the unit, ensuring efficient operations and adherence to this SOP. Reports directly to the Director of Administration and Operations.
3. Secretary: Provides administrative support to the Head of Unit, managing schedules, correspondence, and meetings. Handles day-to-day administrative tasks. Reports to the Head of Unit.
4. Administrative Officer: Assists the Secretary, handles routine administrative tasks, and may lead specific projects as assigned. Reports to the Head of Unit.
5. Clerical Officer: Manages mail, documents, and filing systems, ensuring accurate record-keeping. Reports to the Head of Unit.
6. Storekeeper: Maintains inventory of unit supplies and equipment, manages procurement processes (in accordance with University policy), and ensures proper storage and security. Reports to the Head of Unit.
7. Systems Analyst: Supports the Head of Unit in analyzing the performance of other COMSIT units, providing data-driven insights to improve efficiency. Reports to the Head of Unit.

IV. OPERATIONAL PROCEDURES:

1. Communication: A centralized communication system (e.g., shared drive, collaboration software) must be used for all official communication within the unit and with other COMSIT units. Clear communication protocols (including response times) will be established and regularly reviewed. Regular team meetings, shall be held.
2. Document Management: A robust document management system (DMS) will be implemented to store, manage, and access all unit documents. Access control will be

strictly enforced, following University IT security policies. Version control and an archiving system will be in place. The DMS should conform to University standards for document retention and disposal.

3. Project Management: The unit will adopt a formal project management methodology (e.g., Agile, Waterfall) for managing all projects. Projects will be initiated with a clear scope, timeline, budget, and assigned team members. Progress will be tracked and reported regularly. This includes documenting decisions, risks, and potential issues.
4. Risk Management: A process for identifying, assessing, and mitigating risks to unit operations will be established and regularly reviewed. The unit will develop and implement a risk register, updated and monitored regularly.
5. Performance Measurement: Key Performance Indicators (KPIs) from the provided blueprint will be tracked and reported regularly (monthly or quarterly reports). This data will inform continuous improvement initiatives. KPIs should be tied to strategic objectives defined by the Director of Administration and Operations.
6. Escalation Procedures: A clear escalation path is defined for issues and problems (see Line of Command above). Any issues not immediately resolvable by the designated staff should be escalated to the next level of responsibility in a timely fashion. This will ensure efficient problem-solving.
7. Training and Development: Staff will receive regular training to maintain proficiency in relevant software, systems, and administrative procedures. This will include training on new technologies, security protocols, and best practices in university administration.
8. Compliance: The unit will strictly adhere to all relevant University policies, procedures, and regulations regarding finance, IT security, data privacy, and human resources.

I. LINE OF COMMAND

Administrations

1. : Overall responsibility for unit administration and operations
2. Unit Head: Deputize for Director
3. Secretary: Support the chairperson and oversees administrative tasks.
4. Administrative Officer: Assists the Secretary and handles day-to-day administrative duties

Operations

1. Director of Operations: Oversees unit operations and implements strategic plans.
2. Program Manager: Responsible for specific programs or projects within unit.
3. Operation Officer: Support program managers and handle operational tasks
4. Human Resources Department: Oversees recruitment, training, and personnel management
5. Information Technology Department: Manages IT/ infrastructure, systems, and support
6. Steering Committee: Provides strategic guidance and oversight.

7. Technical Committee: Provides technical expertise and advice

J. DOCUMENT CONTROL

1. Version:
2. Effective Date:
3. Review Due Date:
4. Prepared by:
5. Approved by:
6. Distribution:

Document Control Procedure

1. Document Creation - create documents by authorized personnel using approved format
2. Document Review
3. Document Distribution
4. Document Storage
5. Document Revision
6. Document Retirement

K. FUTURE EXPANSION PLAN

1. Increase Staff Capacity: Recruit additional staff to support growing administrative needs
2. Implement a Document Management System: Introduce a robust document management system to streamline document storage

L COMMUNICATION PLAN

The proposed strategies for a comprehensive communication plan to manage communication within the various units under the Deputy Director, Administration and Operations, as well as with other departments are:

1. Establish Communication Channels and Protocols
    1. Define communication channels (e.g., email, instant messaging, video conferencing) for different types of communication (formal, informal, urgent, non-urgent).
    2. Develop communication protocols and guidelines for each channel, including response times, message formatting, and appropriate use.
    3. Ensure all staff members are aware of and trained on the communication channels and protocols.

2. Implement a Centralized Communication Platform

    1. Adopt a centralized communication platform (e.g., collaboration tools) to facilitate communication and information sharing within and across units.
    2. Provide training and support to staff on the effective use of the platform.
    3. Encourage the use of the platform for project coordination, document sharing, and knowledge management.

3. Regular Meetings and Updates

    1. Schedule regular team meetings within each unit to discuss progress, challenges, and upcoming tasks.
    2. Organize cross-functional meetings or workshops for units working on interdependent projects or initiatives.
    3. Conduct weekly or bi-weekly updates with unit heads/coordinators to ensure alignment and communication flow.

4. Establish a Crisis Communication Plan

    1. Develop a crisis communication plan to manage communication during unexpected events, emergencies, or incidents.
    2. Define communication protocols, roles, and responsibilities in crisis situations.
    3. Identify key stakeholders and communication channels for crisis communication.

5. Implement a Feedback Mechanism

1. Establish channels (e.g., surveys, suggestion boxes, town hall meetings) for staff and stakeholders to provide feedback and suggestions.
2. Regularly review and analyze feedback to identify areas for improvement in communication and operations.
3. Communicate actions taken based on feedback to foster transparency and trust

6. Communication Skills Development

1. Provide training and development opportunities for staff to enhance their communication skills (e.g., written, verbal, presentation, active listening).
2. Encourage participation in internal and external communication-related workshops or seminars.
3. Foster a culture of open and effective communication through leadership support and recognition.

M. COMMUNICATION PROTOCOL

1. Formal Communication
    1. Email
    2. Memoranda
    3. Letters
2. Informal Communication
    1. Instant Messaging
    2. Phone calls
3. Communication Channels

Newsletter: newsletter will be published regularly to share updates and information with the university community.

N. INTERFACING AREAS WITH OTHER COMSIT UNITS:

Collaborate with related units to ensure cohesive development and implementation strategies.

O CONCLUSION

The Deputy Director, Administration and Operations, stands as the conductor, harmonizing the diverse talents and resources within the COMSIT Directorate. As the institution embarks on its digital transformation journey, the Deputy Director's leadership and vision will be instrumental in orchestrating a harmonious convergence of technology, talent, and innovation. By embracing the strategies outlined in this blueprint, this will unlock new realms of efficiency, resilience, and digital eminence, positioning the institution as a trailblazer in the ever-evolving digital landscape.

CYBERSECURITY AND MULTIMEDIA UNIT

A. OPERATIONAL BRIEF

The unit shall oversee the security and protection of university's digital assets and resources by identifying the assets, categorizing them in order of security risk level and suggest the best cyber security approach for implementation. The unit shall also be responsible from time to time analysis of potential threats through regular report to the Director for likely attack mitigation strategies. The unit shall also coordinate all multimedia implementations within the University in line with the University's established procedures and ICT policy. The unit is dedicated to ensuring the confidentiality, integrity, and availability of the University's digital asset information systems and resources.

B. INTRODUCTION

The cybersecurity unit was never in existence before now. It is just being conceived in order to have a secured and user trusted environment for university ICT ecosystem. The following are some of the potential benefits for the university community:

i. **Stronger Cybersecurity Posture**: This initiative will promote University of Ilorin through adequate protection of her digital assets, information system and resources.

ii. **Proactive Cybersecurity Measures:** The unit can actively search for weaknesses and unusual activities in systems, enabling the gathered security information to mitigate security threats.

1. **Continuous threat hunting:** By constantly monitoring systems, the unit shall act as a security lookout (security eagle eye), identifying and addressing potential dangers before they can cause harm.
2. **Early warning system for security:** the cybersecurity unit functions like an early warning system for security issues, allowing them to be dealt with before they turn into major problems.
3. **Developing in-house Cybersecurity Capacity:** Through necessary workshops and training on best practices like recognizing phishing attempts and creating strong passwords, the unit shall equip her personnel to be the first line of defense against security threats and attacks.
4. **Promoting University-wide Cybersecurity Awareness:** By implementing training programs, the cybersecurity unit is expected to fosters a culture where members of the university community are aware of cyber threats and take steps to minimize security risks.

C. MISSION STATEMENT

Mission: To promote confidentiality, integrity and availability of the digital assets, information systems and resources within the university's ICT ecosystem and to be the frontier in providing innovative and high-quality multimedia services, empowering teaching, learning, research, and community engagement at the University of Ilorin.

D. STAFFING:
Personnel:
Core Team:

1. **Head of Unit** -Chief Information and Cybersecurity Officer (CISO)(1): Oversees all cybersecurity operations by developing appropriate strategies and framework to secure university digital assets, information systems and resources.

Technical Team

1. **Cybersecurity Analysts**: Monitor security systems, analyze logs, investigate security incidents, and perform vulnerability assessments.
2. **Cybersecurity Engineers**: Design, implement, and maintain security infrastructure, including firewalls, intrusion detection systems, and security information and event management (SIEM) systems. Conduct ethical hacking exercises to identify vulnerabilities in systems and applications. Investigate cybercrimes and collect digital evidence.
3. **Cybersecurity Architects**: Design and implement secure network architectures and security solutions.

Support Team

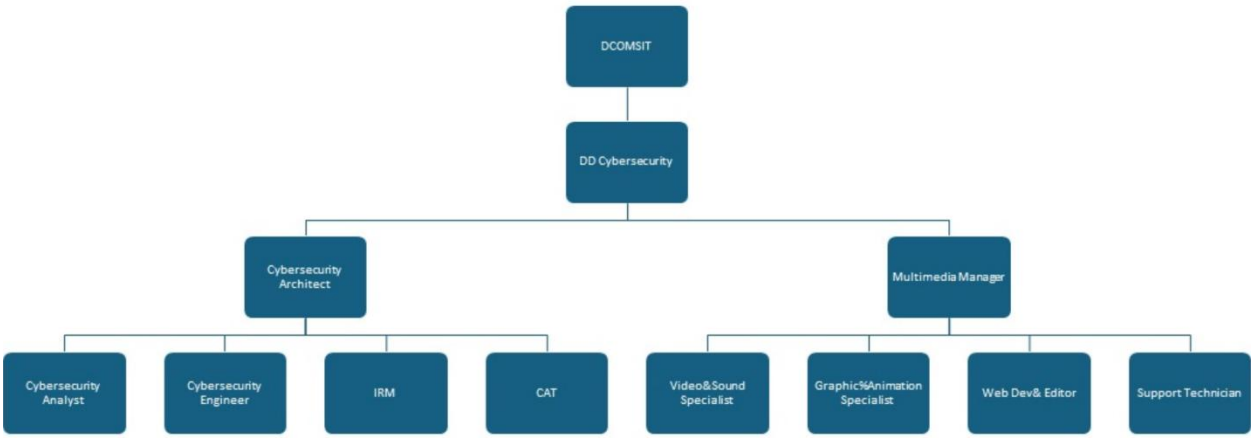
1. **Security Awareness Trainers**: Develop and deliver security awareness training programs to educate faculty, staff, and students.

The Multimedia Unit is a sub -unit of cybersecurity unit and will require a dedicated team reporting to the head of cybersecurity and multiunit. A staffing as shown below is recommended.

Staffing Multimedia

1. Multimedia Manager
2. Video Production Specialist and sound engineer
3. Graphic Designer/ Animation Specialist
4. Web Developer/Content editor
5. IT Support Technician (dedicated to multimedia infrastructure)

E. **UNIT ORGANOGRAM**



F. S**WOT ANALYSIS**

Strength: Due to nonexistence of this unit before now, the current cybersecurity posture of university needs to undergo a thorough review in terms of potential threats, risks as well as mitigation strategies around the university digital assets with an inherent motive to emerge with information Security Policy document. The Information Security policy shall:

1. **Defines Security Guidelines:** ICT Security policy shall establish clear guidelines on how employees and authorized users should interact with the organization's ICT systems.
2. **Protection of digital Assets:** By outlining security measures, the policy helps safeguard the organization's valuable information assets, such as customer data, financial records, and intellectual property.
3. **Ensures Compliance:** Many industries have regulations regarding data privacy and security, the policy is expected to address this as well.
4. **Promotes Security Awareness:** The document serves as a reference point for employees to understand the organization's commitment to cybersecurity and their individual responsibilities in maintaining it.
5. **Provides Framework for Incident Response:** Due to the likelihood of occurrence of date breaches or other common potential incidence, the policy shall establish guidelines for how to identify and respond to security incidents.

Weakness: The absence of a cybersecurity unit is similar to having a sleeping watchdog guarding your valuables. They are unaware of potential threats, leaving the university vulnerable to cyber attacks. Below are some additional danger/weakness in such a system:

1. **Reactive Nature:** the sort of organization is seen to be unprepared as known dangers are apparently being taken for granted, thereby increasing the potential devastating impact of the digital assets and making the recovery process become difficult if not impossible to achieve.
2. **Slow Response Times:** In the event of a cyber attack, the lack of a trained response team can lead to delayed detection. This allows attackers to have more time to infiltrate systems, steal data, or cause disruption.
3. **Lack of Awareness and Training:** Employees are often the first line of defense against cyber threats. However, without proper education and training on cybersecurity best practices, they might be more susceptible to phishing scams, social engineering attacks, or unknowingly downloading malware.
4. **Inconsistent Security Measures:** Without a centralized unit overseeing security, security practices might be inconsistent across the university. This creates a patchwork defense that attackers can exploit.
5. **Compliance Risks:** Many industries have regulations regarding data security. The absence of a dedicated cybersecurity unit can make it difficult for the university to comply with these regulations, potentially leading to legal or financial penalties.

Opportunities: Additional benefits of having a dedicated cybersecurity unit in the university includes:
Securing the Future of Innovation: Research data and intellectual property are the cornerstone of a university's innovative spirit. A cybersecurity unit acts as a shield, preventing unauthorized access and data breaches that could have crippling financial and poor corporate image. This is paramount for universities engaged in pioneering research endeavors.

Think Tank for Shared Defense: The unit fosters a collaborative environment where researchers, faculty, and students can work together on cybersecurity challenges. This synergy of minds can lead to groundbreaking research and the development of advanced security solutions that protect the entire academic community.

Secure User Interaction:

1. **Building a Security-Conscious Culture:** By promoting cybersecurity awareness through training programs and initiatives, the unit can cultivate a culture of responsible digital behavior among students, faculty, and staff. This equips everyone to navigate the online world safely and protects their personal information.
2. **Improved Cybersecurity Awareness:** The unit shall develop programs to educate students on cybersecurity best practices, such as recognizing phishing scams, creating

strong passwords, and practicing safe social media habits. This empowers students to be their own first line of defense against cyber threats.

Stronger Cybersecurity Infrastructure:

1. **Digital Assets:** The unit continuously monitors the university's IT infrastructure for vulnerabilities and suspicious activity.
2. **Compliance and Risk Management:** Many industries, including education, have regulations regarding data security. The cybersecurity unit can help the university ensure compliance with these regulations, mitigating potential legal or financial penalties.

Additional Opportunities:

1. **Incident Response and Recovery:** The unit shall establish protocols for identifying, containing, and recovering from cybersecurity incidents. This minimizes downtime and ensures a swift and effective response to security threats.
2. **Community Outreach:** The unit can extend its expertise beyond the university walls, offering cyber ecurity awareness programs to local businesses and communities. This fosters a collaborative approach to cybersecurity in the broader region.

Threats: As an enterprise organization, with most of her operations revolves around the web, there is every possibility of potential threats arising from intrusion, phising, code vulnerability, unauthorized access etc. Which can have negative security implication on student record, research data, staff record, intellectual properties as well as university classified documents and primary data.

The consequences of these cybersecurity threats can be severe to the university, leading to:

1. **Financial Losses:** From paying ransoms to repairing damage caused by attacks and complying with data breach regulations.
2. **Reputational Damage:** Loss of trust from students, parents, faculty, and donors can have a long-term impact on a university's reputation.
3. **Disruption of Operations:** Cyber attacks can disrupt online learning platforms, administrative systems, and research projects, hindering the university's core functions.
4. **Loss of Intellectual Property:** Data breaches can expose valuable research data and intellectual property, giving competitors an unfair advantage.

Thus, a functional cybersecurity framework is capable of mitigating such threats.

Multimedia Unit SWOT Analyses

Strengths	Weaknesses	Opportunities	Threats
Existing ICT Directorate infrastructure and expertise	Limited initial budget and resources	Growing demand for multimedia content in education	Rapid technological advancements requiring continuous investment
University's diverse faculties and centers providing a wide range of content possibilities	Potential lack of skilled personnel in specialized multimedia areas	Partnerships with external organizations for funding and expertise	Resistance to change from traditional teaching methods
Strong university brand and reputation	Potential for equipment obsolescence	Development of online learning platforms and MOOCs	Data security and privacy concerns
Established network infrastructure	Potential for internal bureaucratic hurdles	Generation of revenue through multimedia services	Power outages and unreliable internet connectivity

G. **KEY PERFORMANCE INDICATORS (KPIS)**

Here are some key performance indicators (KPIs) to measure the success of the university cybersecurity unit:

Risk Management:

1. **Number of vulnerabilities identified and remediated:** Tracks progress in patching vulnerabilities and reducing security risks.
2. **Mean Time to Remediate (MTTR) vulnerabilities:** Measures the average time it takes to patch vulnerabilities after discovery(time between when the vulnerability was discovered and resolved).
3. **Number of Cybersecurity incidents:** Indicates the overall frequency of security events.
4. **Cost of Cybersecurity incidents (if applicable):** Helps quantify the financial impact of security breaches.
5. **Cybersecurity Awareness:** measuring the level of cybersecurity awareness among members of the university community using surveys and simulations
6. **Number of reported suspicious activities:** Indicates user vigilance and willingness to report potential security threats.
7. **Detection and Response:**
8. **Number of security alerts investigated:** Tracks the unit's responsiveness to potential security incidents.

9. **Mean Time to Detection (MTTD) of security incidents:** Measures the average time it takes to identify a security incident.
10. **Mean Time to Respond (MTTR) to security incidents:** Measures the average time it takes to contain and remediate a security incident.
11. **Compliance:** with external frameworks
12. **Number of security policy violations:** Tracks adherence to established security policies and procedures.
13. **Compliance with external regulations (e.g. NIST, ISMS):** Ensures the university meets relevant data privacy requirements.
14. **Overall Program Effectiveness:**
15. **Return on Investment (ROI) of cybersecurity initiatives (if quantifiable):** Demonstrates the value of cybersecurity investments in terms of cost savings or risk reduction.
16. **User satisfaction with Cybersecurity measures:** Gathers user feedback on the perceived effectiveness and user-friendliness of security controls.
17. **Additional Considerations:**
18. Choose KPIs relevant to the university's specific security goals and risk profile.
19. Regularly monitor and track KPIs to identify trends and areas for improvement.
20. Report on KPIs to university leadership to demonstrate the cybersecurity unit's value.

Key Performance Indicators (KPIs): Multimedia

- **Service Availability:** Uptime of multimedia equipment and online platforms.
- **Content Creation:** Number of videos, graphics, and other multimedia resources produced.
- **User Satisfaction:** Feedback from faculty, students, and staff on the quality of services.
- **Training & Support:** Number of training sessions conducted and users supported.
- **Project Completion Rate:** Percentage of multimedia projects completed on time and within budget.
- **Infrastructure Utilization:** Usage rates of multimedia equipment and facilities.
- **Website Traffic & Engagement:** Metrics for online multimedia content.

H. STANDARD OPERATIONS PROCEDURE (SOP)

Cybersecurity:

A. Incident Response:

1. **Detection:** Any suspected security incident (e.g., phishing email, malware detection, unauthorized access) must be immediately reported to the Cybersecurity Analyst via the designated reporting channels (email, phone, ticketing system).

2. **Initial Response:** The Cybersecurity Analyst follows the incident response plan, prioritizing containment and minimizing further damage. Initial actions may include isolating affected systems, blocking malicious traffic, and preserving evidence.
3. **Investigation:** A full investigation is conducted to determine the incident's root cause, scope, and impact. This may involve collaborating with other ICT units and external forensic experts.
4. **Remediation:** Necessary steps are taken to eliminate the vulnerability and restore the affected systems to a secure state.
5. **Recovery:** Systems and data are restored to their pre-incident state.
6. **Post-Incident Activity:** A post-incident report is compiled, documenting the incident details, root cause, remediation steps, and lessons learned. This report is reviewed by the unit head and shared with relevant stakeholders.
7. **Escalation:** Any critical incidents (those posing significant risk or requiring extensive resources) are escalated to the unit head and the appropriate university leadership.

B. Vulnerability Management:

1. **Vulnerability Scanning:** Regular vulnerability scans of university systems are performed by the IT Security Specialist using automated tools.
2. **Assessment and Prioritization:** Identified vulnerabilities are assessed based on their severity and potential impact.
3. **Remediation:** Remediation actions (e.g., patching, configuration changes, security controls) are implemented by the IT Security Specialist or other relevant teams.
4. **Verification:** Remediation efforts are verified to ensure vulnerabilities are effectively addressed.
5. **Reporting:** Vulnerability scan results and remediation progress are reported to the unit head on a regular basis.

C. Security Awareness Training:

1. **Program Development:** The Security Awareness Trainer develops and delivers regular training programs on cybersecurity best practices (phishing awareness, password management, data security). Training programs should be tailored to different user groups (faculty, staff, students).
2. **Training Delivery:** Training is delivered through various methods (online modules, workshops, presentations).
3. **Evaluation:** Training effectiveness is evaluated through assessments, phishing simulations, and post-training surveys.
4. **Updates:** Training materials are regularly updated to address new threats and vulnerabilities.

Multimedia

Standard Operating Procedures (SOP) for the Multimedia Unit

This document outlines the Standard Operating Procedures (SOP) for the Multimedia Unit at the University of Ilorin, detailing responsibilities and workflows for each role.

I. Multimedia Manager

1. **Overall Responsibility:** Oversees all operations of the Multimedia Unit, ensuring efficient service delivery and alignment with university objectives.
2. **Key Procedures:**
    1. **Project Management:**
        1. Receives project requests from faculties/centers.
        2. Assigns projects to relevant team members.
        3. Monitors project progress and ensures timely completion.
        4. Manages project budgets and resources.
        5. Conducts project evaluations and gathers feedback.
    2. **Staff Management:**
        1. Supervises and evaluates team performance.
        2. Conducts regular team meetings.
        3. Identifies training needs and facilitates professional development.
        4. Manages staff schedules and leave requests.
    3. **Strategic Planning:**
        1. Develops and implements the unit's strategic plan.
        2. Sets performance targets and monitors KPIs.
        3. Identifies opportunities for growth and expansion.
        4. Prepares reports on unit activities and performance.
    4. **Budget Management:**
        1. Develops and manages the unit's budget.
        2. Approves expenditures and tracks expenses.
        3. Identifies funding opportunities and prepares grant proposals.

5. **Policy Development:**

    1. Develops and implements policies and procedures for the unit.
    2. Ensures compliance with university regulations.

6. **User Relationship Management:**

    1. Maintains strong relationships with faculty and center representatives.
    2. Addresses user concerns and resolves issues.

II. Video Production Specialist & Sound Engineer

1. **Overall Responsibility:** Responsible for all aspects of video production, from pre-production planning to post-production editing and sound design.
2. **Key Procedures:**
    1. **Pre-Production:**
        1. Meets with clients to discuss project requirements.
        2. Develops storyboards and scripts.
        3. Scouts locations and arranges logistics.
        4. Selects and manages video equipment.
    2. **Production:**
        1. Operates cameras and other recording equipment.
        2. Directs on-camera talent.
        3. Ensures proper lighting and sound recording.
    3. **Post-Production:**
        1. Edits video footage using professional editing software.
        2. Adds special effects and graphics.
        3. Creates sound design and mixes audio tracks.
        4. Ensures high-quality video and audio output.
    4. **Sound Engineering:**
        1. Records and edits audio for various multimedia projects.
        2. Sets up and operates sound equipment.
        3. Designs and mixes sound effects and music.
        4. Ensures high-quality audio output.

III. Graphic Designer/Animation Specialist

1. **Overall Responsibility:** Creates visually appealing graphics and animations for various multimedia projects.
2. **Key Procedures:**
    1. **Graphic Design:**
        1. Develops visual concepts and designs.
        2. Creates logos, posters, brochures, and other marketing materials.
        3. Designs website layouts and graphics.
        4. Uses graphic design software effectively.
    2. **Animation:**
        1. Creates 2D and 3D animations.
        2. Develops storyboards and animatics.
        3. Uses animation software and techniques.
        4. Ensures high-quality animation output.
    3. **Branding:**
        1. Maintains university brand guidelines in all designs.
        2. Ensures consistency in visual communication.

IV. Web Developer/Content Editor

1. **Overall Responsibility:** Develops and maintains the unit's website and manages multimedia content.
2. **Key Procedures:**
    1. **Web Development:**
        1. Designs and develops websites using web development tools.
        2. Ensures website functionality and responsiveness.
        3. Manages website hosting and maintenance.
    2. **Content Management:**
        1. Creates and edits website content.
        2. Manages multimedia files and uploads them to the website.
        3. Ensures website content is accurate and up-to-date.
    3. **SEO:**
        1. Implements search engine optimization (SEO) best practices.
        2. Monitors website traffic and analytics.
    4. **Accessibility:**
        1. Ensures website accessibility for users with disabilities.

V. IT Support Technician (1)

1. **Overall Responsibility:** Provides technical support for the Multimedia Unit's infrastructure and equipment.
2. **Key Procedures:**
    1. **Equipment Maintenance:**
        1. Maintains and repairs multimedia equipment.
        2. Troubleshoots technical issues.
        3. Ensures equipment is in good working order.
    2. **Network Support:**
        1. Manages the unit's network infrastructure.
        2. Troubleshoots network issues.
        3. Ensures network security.
    3. **Software Support:**
        1. Installs and configures software.
        2. Provides software support to team members.
    4. **Help Desk:**
        1. Provides technical support to users of multimedia services.
        2. Logs and tracks support requests.
    5. **Inventory Management:**
        1. Maintains an inventory of multimedia equipment and supplies.
        2. Tracks equipment usage and maintenance records.

VI. General Procedures:

1. **Project Request Process:** A standardized form for requesting multimedia services will be available online and in print. The form will include project details, timeline, and budget requirements.
2. **Communication:** Regular team meetings will be held to discuss project progress, address challenges, and share updates. Email and other communication tools will be used for day-to-day communication.
3. **Quality Control:** A quality control process will be implemented for all multimedia projects to ensure high standards and client satisfaction.
4. **Data Backup:** A regular data backup process will be implemented to protect multimedia files from loss or damage.
5. **Security:** Security measures will be implemented to protect multimedia equipment and data from theft or unauthorized access.

D. Policy and Compliance:

1. **Policy Development and Review:** The Cybersecurity Unit is responsible for the development and regular review of the University's information security policies and procedures.
2. **Compliance Monitoring:** Compliance with relevant data protection regulations and industry best practices is ensured.
3. **Audits:** Regular security audits are performed to assess the effectiveness of security controls and compliance with policies.
4. **Reporting:** Reports on policy compliance and audit results are submitted to the unit head and relevant university bodies.

. **LINE OF COMMAND(top-down)**

Cybersecurity:

1. Director of COMSIT
2. Unit Head Cybersecurity and multimedia
3. Cybersecurity Architects
4. Cybersecurity Engineers/Analyst
5. Security Awareness Trainers
6. Individual volunteers (Non Expert, interest group, etc.)

Multimedia

1. Director of COMSIT
2. Unit Head Cybersecurity and multimedia
3. Multimedia Manager
4. Video Production Specialist and sound enginer
5. Graphic Designer/ Animation Specialist
6. Web Developer/Content editor
7. IT Support Technician

J. DOCUMENT CONTROL

1. Version:
2. Effective Date:
3. Review Due Date:
4. Prepared by:
5. Approved by:
6. Distribution:

1. Types of Documents:
2. Requirements Specifications
3. Design Documents
4. Test Plans and Reports
5. User Manuals
6. Change Requests

7. Revision history

2. Version Control System (tracking, back up, etc):
    1. Implement a version control system to manage document versions, changes, and collaboration.

3. Document Approval Process:
    1. Define a clear approval workflow for documents, including review cycles and sign-off procedures.

4. Access Control:
    1. Establish access permissions to ensure that only authorized personnel can view, edit, or approve documents.

5. Document Storage and Retrieval:
    1. Utilize a centralized document repository with a logical structure for easy storage, retrieval, and searchability.

K. FUTURE EXPANSION PLANS

Cybersecurity unit

1. New Technology Adoption:
2. Stay abreast of emerging technologies and trends to incorporate innovative solutions into development processes.
3. Capacity and Human Resource Development:
4. Invest in training programs to upskill team members and equip them with the latest tools and techniques.
5. Collaboration with Research Institutions:
6. Explore partnerships with research institutions to leverage cutting-edge research for new software development approaches.
7. International Collaboration:
8. Foster collaborations with international counterparts to exchange knowledge, best practices, and foster cross-cultural understanding.

Multimedia unit

1. **Multimedia Learning Centers:** Establish dedicated spaces in faculties and centers equipped with multimedia technology.
2. **Mobile Multimedia Unit:** A mobile unit for on-location recording and events.
3. **Partnerships:** Collaborate with external organizations for funding, expertise, and technology.
4. **Research and Development:** Explore new multimedia technologies and their applications in education.

L. COMMUNICATION PLANS

1. Internal Communication:

1. Regular team meetings to discuss project updates, challenges, and achievements.
2. Utilize collaboration tools (e.g. Microsoft Teams) for real-time communication and file sharing.
3. Quarterly unit meetings to share updates and gather feedback from team members.
4. Regular update on new technology and emerging innovative devices to improve quality of multimedia service delivery.

2. External Communication:

1. Establish a dedicated email address and contact point for external inquiries and feedback.
2. Maintain an active presence on social media platforms to showcase projects, achievements, and job opportunities.
3. Participate in industry events, conferences, and webinars to network and promote the unit's capabilities.

M. COMMUNICATION PROTOCOL

1. Email Communication:

1. Use clear and concise language in email communication.
2. Include relevant subject lines and action items for quick reference.
3. Follow up on important emails to ensure timely responses.

2. Hard copy memoranda:

1. Establish a standardized format for hard copy paper memos, including headings, date, recipients, sender's name, and signature fields, etc.

a. Distribution List:

1. Maintain an up-to-date distribution list for paper memos to ensure that the right individuals receive the information in a timely manner.

b. Tracking and Recording:
Implement a system for tracking and recording the distribution of paper memos, including acknowledgement of receipt and any follow-up actions required.
c. Enforce strict confidentiality measures for sensitive information included in paper memos, such as handling procedures and secure storage.
d. Archiving and Retention: Establish guidelines for the archiving and retention of paper memos, including storage duration and disposal procedures in compliance with data protection regulations.
e. Version Control: Maintain version control for paper memos by including a version number or date to ensure that the most recent information is being referenced.

3. Meeting Etiquette:
    1. Start meetings on time and adhere to the agenda to maximize productivity.
    2. Assign roles (e.g., facilitator, timekeeper) to ensure efficient meeting management.
    3. Encourage active participation and respectful dialogue among team members.
4. Feedback Mechanisms:
    1. Implement regular feedback sessions to gather input on communication effectiveness and areas for improvement.
    2. Provide avenues for anonymous feedback to encourage candid responses.
    3. Act on feedback promptly to address concerns and enhance communication practices.

N. INTERFACING AREAS WITH COMSIT UNITS AND UNIVERSITY COMMUNITY

This communication plan outlines strategies for informing university stakeholders (faculty, staff, students, management and relevant organs of the COMSIT) about the cybersecurity landscape and its implications for the university. Effective communication fosters awareness, promotes responsible behavior, and strengthens the overall cybersecurity posture and assures that the university is pro-active.

Target Audiences:

1. **COMSIT Director:** Present a comprehensive overview of the cybersecurity landscape, risks facing the university, and mitigation strategies implemented by the cybersecurity unit.
2. **COMSIT Units:** this is of great priority for the relevant Units of COMSIT to be adequately informed about the activities of the cybersecurity at all time. A robust and real time information sharing platform should be developed to foster seamless vertical and horizontal exchange of cybersecurity incidents as well activities for ease of monitoring.
3. **Staff:** Educate them on common cyber threats, best practices for protecting university data, and reporting procedures for suspicious activity.
4. **Students:** Raise awareness of cyber risks they may encounter, guide them on secure online behavior, and emphasize responsible use of university IT resources.

Collaboration with Faculties and Centers on Multimedia Innovations

5. Establish liaison officers in each faculty and center to facilitate communication and identify multimedia needs.
6. Conduct regular meetings with faculty representatives to gather feedback and ensure alignment with their requirements.
7. Offer customized training and support to faculty and staff on using multimedia tools and resources.

Communication Channels:

1. **Email Campaigns:** Send regular email campaigns with cybersecurity tips, updates on emerging threats, and reminders about security policies.
2. **Training Sessions:** Organize workshops and training sessions tailored to different stakeholder groups, covering topics like phishing awareness, password hygiene, and data security best practices.
3. **Website:** Create a dedicated webpage on the university website with cybersecurity resources, FAQs, reporting mechanisms for suspicious activity, and contact information for the cybersecurity unit.
4. **Social Media:** Utilize university social media platforms to share cybersecurity awareness messages and promote upcoming training sessions. Other available social platforms can as well be explored for an effective alert system incase of emergency.
5. **Faculty/Staff Meetings:** Incorporate cybersecurity awareness discussions into regular faculty and staff meetings.
6. **Campus Events:** Organize cybersecurity awareness events and campaigns throughout the year to keep the topic at the forefront.
7. **Security incidents Simulation:** this is a systematic approach to evaluate the security posture in order to facilitate further improvement.

Communication Messages:

1. **Tailored Content:** Adapt communication messages to resonate with each stakeholder group. Focus on the specific risks and responsibilities relevant to each audience.
2. **Clear and Concise Language:** Avoid overly technical jargon. Use clear and concise language that everyone can understand.
3. **Focus on Impact:** Highlight the potential consequences of cyber attacks on the university and individuals (data breaches, privacy violations, disruptions).
4. **Call to Action:** Clearly outline the desired actions stakeholders should take to improve cybersecurity (participate in training, report suspicious activity, practice secure online habits).
5. **Positive Reinforcement:** Recognize and appreciate faculty, staff, and students who demonstrate responsible online behavior and report suspicious activity.

Shared Resources and Expertise:

1. **Cross-training Opportunities:** Provide opportunities for staff in different ICT units to receive cross-training on cybersecurity basics and relevant security tools.
2. **Shared cybersecurity Resources:** Maintain a central repository of security resources, best practices documents, and incident response procedures accessible to all ICT units.
3. **Joint cybersecurity Projects:** Collaborate on security projects that benefit the entire university, such as implementing multi-factor authentication or data encryption across all ICT systems.
4. **Code vulnerability expert:** also known as a security analyst, security engineer, or penetration tester, is a cybersecurity professional who specializes in identifying and mitigating security weaknesses in software code. They possess a deep understanding of programming languages, software development practices, and common security vulnerabilities.

Alignment with ICT Directorate Goals and strategies of ISMS:

1. **Understand Directorate Goals:** The cybersecurity unit should understand the overall goals and priorities of the ICT directorate. This helps tailor security strategies to support and not hinder the directorate's objectives.
2. **Risk-Based Approach:** Prioritize cybersecurity efforts based on risks identified across the university, considering systems and data managed by other ICT units.
3. **Security Champions:** Identify and empower security champions within other ICT units to promote security awareness and best practices among their colleagues.
4. **Benefits of Congruence:**
5. **Improved Security Posture:** Collaboration and information sharing lead to a more comprehensive and effective security posture for the university.
6. **Reduced Risk of Cyber Attacks:** A unified approach to security makes the university less vulnerable to cyberattacks.
7. **Enhanced Efficiency:** Integration and automation can streamline security processes and reduce duplication of effort across ICT units.
8. **Improved Communication:** Clear communication fosters trust and collaboration between the cybersecurity unit and other ICT units.

By fostering a collaborative and integrated approach, the cybersecurity unit can achieve congruence with other units within the ICT directorate, leading to a more secure and resilient university IT environment.

O. Conclusion:

This document has provided a deep insight to the blueprint for university of Ilorin cybersecurity unit with focus on development on plans to attain some long term plans. The document is based on best practices in the global IT sector using the principles in Information Security Management System ISMS and The National Institute of Standards and Technology (NIST) frame works.

DIGITAL INNOVATIONS AND ICT IDEATION UNIT

. OPERATIONAL BRIEF

The unit shall coordinate the digital innovations drive of the. University from conception of the idea to the implementation stage and even evaluation of the impact of such digital innovation on the University's core processes.

A. INTRODUCTION

The responsibility of a Digital Innovations and ICT Ideation Unit in a university typically revolves around fostering technological innovation and leveraging information and communication technology (ICT) to enhance various aspects of the university's operations and academic endeavors.

C: MISSION STATEMENT:

To drive cutting-edge digital transformation by fostering creativity, collaboration, and innovative ICT solutions, through innovative thinking and ideation empowering organizations to thrive in an ever-evolving technological landscape.

D: STAFFING:

Unit Head: Leads the overall strategy, vision, and operations of the unit. And also ensures alignment with organizational goals and drives innovation

ICT Strategist: Develops long-term strategies for integrating digital solutions and emerging technologies and to guide decision-making in the unit.

Digital Innovation Manager: Helps in Identifying new innovation/ opportunities that elevates the digital transformation of the unit.

ICT Solutions Architect: Designs and architects adaptable, secure, and innovative ICT systems. And ensures the digital solution aligns with business needs.

Innovation Researcher: Provides insights and data-driven recommendations for future innovation.

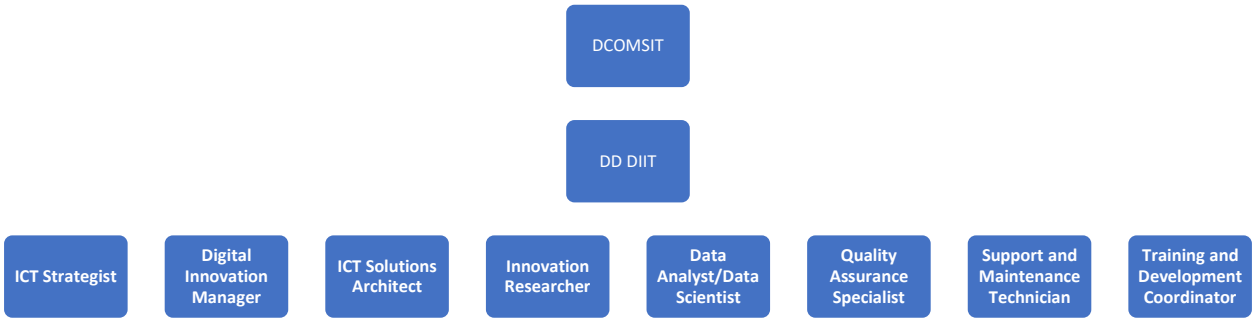
Data Analyst/Data Scientist: Collects, analyzes, and interprets data to provide insights that guide digital strategy that helps in good decision making.

Quality Assurance Specialist: Conducts testing to ensure that digital products meet quality standards to make end-users experience seamless and smooth.

Support and Maintenance Technician: Provides ongoing support and troubleshooting for digital solutions and ensures the system remains functional.

Training and Development Coordinator: Overseas training, training materials and required sessions for both internal and external teams.

E. UNIT ORGANOGRAM:



F. SWOT ANALYSIS

STRENGTHS:

1. Access to skilled professionals with deep technical knowledge in digital innovation and ICT ideation.
2. Ability to generate executable ideas and develop groundbreaking digital products that meet the digital needs.

3. Flexible and quick in adapting to technological changes and transformations.

WEAKNESS:

1. High rate of staff mobility in the field of ICT.
2. Focus on advanced technologies may result in solutions that are complex or not aligned with immediate business needs.
3. Heavy dependence on third party platform which can eventually limit flexibility

1.

OPPORTUNITY:

1. Increasing demand for digital transformation in various sectors creates opportunities for growth.
2. Opportunities for collaboration with tech startups, universities, or external innovation hubs to accelerate development.
3. Rapid advancement in other ICT sectors offer new possibilities for disruptive innovation.

THREATS:

1. Constant technological advancements could make current solutions outmoded quickly**.**
2. Increased adoption of digital solutions exposes the unit to potential security breaches and data privacy concerns.
3. Growing competition from other organizations or consultancies offering similar digital and ICT innovation services.

G.KEY PERFORMANCE INDICATORS(KPI)

Key performance indicators (KPIs) for a Digital Innovation and ICT Ideation Unit in a university can vary depending on its specific goals, but here are some common metrics to consider:

1. **ICT Strategist:**

KPI: Strategy Development: Percentage of digital strategies implemented successfully.

KPI: Technology Trends: Ability to identify and integrate emerging technologies into the strategy.

0. **Digital Innovation Manager:**

KPI: Innovation Adoption Rate: Rate at which new products/technologies are adopted by end users or clients.

KPI: Project Delivery: Percentage of innovation projects delivered on time and within budget

0. **ICT Solutions Architect:**

KPI:System Performance: Uptime and reliability of designed ICT solutions.
KPI: Scalability and Flexibility: Ability of systems to scale and adapt to new business needs (measured by the number of successful adaptability adjustments).\

0. **Innovation Researcher:**

KPI: Report Timeliness: On-time delivery of research findings and insights to relevant teams
KPI: Adoption of Insights: The percentage of research findings adopted for innovation projects
KPI: Research Quality: Number of relevant and actionable insights derived from research activities.

0. **Data Analyst/Data Scientist:**

KPI: Data Accuracy: Precision of data analysis and insights generated (e.g., error rates in reports etc).
KPI: Model Accuracy: Performance of predictive models (e.g., accuracy, precision).
KPI:Actionable Insights: Number of insights that directly lead to improved business decisions or product enhancements.

0. **Quality Assurance Specialist:**

KPI: Test Coverage: Percentage of the product or system tested before release.
KPI: Bug Detection Rate: Number of issues identified during testing compared to total issues found post-launch.
KPI: User Experience Feedback: End-user feedback on product quality and usability.

0. **Support and Maintenance Technician:**

KPI: Issue Resolution Rate: Percentage of issues resolved on the first attempt.
KPI: System Downtime: Amount of time systems are down due to maintenance or issues.

Training and Development Coordinator:

0. **KPI: Training Effectiveness: Percentage of trainees who successfully apply learned skills on the job.**

KPI: Training Completion Rate: Percentage of employees who complete training programs.
KPI: Training Satisfaction: Feedback from participants regarding the quality and relevance of the training sessions.

H. STANDARD OPERATING PROCEDURE (SOP)

Coordination of Digital Innovations Drive

1. Introduction:

The purpose of this SOP is to provide a clear and structured process for coordinating the digital innovations drive at the University. The unit is responsible for managing the entire lifecycle of digital innovation projects, from idea conception to implementation and evaluation.

2. Objectives:

1. Foster a culture of innovation within the University.
2. Identify and develop digital solutions that enhance the University's core processes.
3. Ensure successful implementation and integration of digital innovations.
4. Evaluate the impact of digital innovations on the University's operations.

3. **Scope:**

This SOP applies to all members of the unit and outlines the procedures for managing digital innovation projects.

4. **Roles and Responsibilities:**

1. Unit Head: Oversees the entire digital innovation drive and ensures alignment with the University's strategic goals.
2. Project Manager: Manages individual digital innovation projects, including planning, execution, and evaluation.
3. Innovation Team: Comprises members with expertise in various digital technologies and processes, responsible for developing and implementing digital solutions.
4. Stakeholders: Includes faculty, staff, and students who provide input and feedback on digital innovation projects.

5. **Procedures:**

5.1 **Idea Conception:**

1. Identify Needs: Conduct surveys, interviews, and workshops to identify areas where digital innovations can enhance the University's processes.
2. Brainstorm Solutions: Organize brainstorming sessions with the innovation team and stakeholders to generate potential digital solutions.
3. Evaluate Ideas: Assess the feasibility, impact, and alignment with the University's strategic goals for each idea.
4. Select Ideas: Prioritize and select the most promising digital innovation ideas for further development.

5.2 **Planning and Development:**

1. Define Project Scope: Clearly outline the objectives, deliverables, and timelines for the selected digital innovation projects.
2. Assemble Project Team: Assign team members based on their expertise and roles within the project.
3. Develop Project Plan: Create a detailed project plan, including milestones, resources, and risk management strategies.
4. Design and Prototype: Develop prototypes and mock-ups of the digital solutions for review and feedback.

5.3 **Implementation:**

1. Execute Project Plan: Follow the project plan and execute tasks as per the defined timelines.
2. Monitor Progress: Regularly track project progress and make necessary adjustments to stay on schedule.
3. Communicate Updates: Provide regular updates to stakeholders on the project's status and any changes
4. Deploy Solution: Implement the digital solution within the University's environment.

5.4. **Evaluation and Impact Assessment:**

1. **Collect Feedback:** Gather feedback from users and stakeholders on the deployed digital solution.
2. **Analyze Impact:** Assess the impact of the digital innovation on the University's core processes, including efficiency, effectiveness, and user satisfaction.
3. **Document Lessons Learned:** Record lessons learned and best practices for future digital innovation projects.
4. **Report Results:** Prepare a comprehensive report on the project's outcomes and impact for review by University leadership.

6. **Continuous Improvement:**

Review SOP: Regularly review and update this SOP to incorporate feedback and improve the digital innovation process.

Encourage Innovation: Foster a continuous culture of innovation by encouraging ongoing idea generation and experimentation.

I. LINES OF COMMAND (TOP-DOWN)

1. Director of COMSIT
2. Unit Head
3. Project Manager
4. Team Leads (ICT Strategist, Data/System Analyst, ICT Solution Architect, Innovation Researcher etc.)
5. Individual Contributors (Digital Innovation Manager, QA Architect, etc.)

J. DOCUMENT CONTROL

Types of Documents:

1. Requirements Specifications
2. Design Documents
3. Test Plans and Reports
4. User Manuals
5. Change Requests

2. Version Control System (tracking, back up, etc):

- Implement a version control system to manage document versions, changes, and collaboration.

3. Document Approval Process:

- Define a clear approval workflow for documents, including review cycles and sign-off procedures.

4. Access Control:

- Establish access permissions to ensure that only authorized personnel can view, edit, or approve documents.

5. Document Storage and Retrieval:

- Utilize a centralized document repository with a logical structure for easy storage, retrieval, and searchability.

K. FUTURE EXPANSION PLAN:

1. Establish a Research and Development (R&D) Hub:

Secure funding and resources to support experimental projects, prototypes, to Create a dedicated space for both internal and external partners to collaborate on cutting-edge ICT research and product development.

2. Develop Industry Partnerships and Collaborations:

Establish joint research projects, internships, and innovation challenges to foster collaboration and knowledge exchange for strategic partnership with tech companies

3. Expand Training and Certification Programs:

Develop online courses, bootcamps, and certificate programs to cater to both university students and external professionals.

4. Develop a Global Innovation Network:

Build a network of global partners for cross-border research projects, exchanges, and knowledge sharing that position the university globally among the leader in digital innovation by collaborating with international institutions and organizations.

5. Enhance Collaboration with Government and Policy Makers:

Engage with government bodies, regulatory agencies, and policymakers to provide expertise and collaborate on digital policy initiatives.

L. Communication Plan:

Internal Communication:

1. Regular team meetings to discuss project updates, challenges, and achievements.
2. Utilize collaboration tools (e.g. Microsoft Teams and other Meeting/Chat platforms) for real-time communication and file sharing.
3. Quarterly unit meetings to share updates and gather feedback from team members.

2. External Communication:

1. Establish a dedicated email address and contact point for external inquiries and feedback.
2. Maintain an active presence on social media platforms to showcase projects, achievements, and job opportunities.
3. Participate in industry events, conferences, and webinars to network and promote the unit's capabilities.

M. COMMUNICATION PROTOCOL:

Communication Protocol

1. Email Communication:

1. Use clear and concise language in email communication.
2. Include relevant subject lines and action items for quick reference.
3. Follow up on important emails to ensure timely responses.

2. Hard copy memoranda:

- Establish a standardized format for hard copy paper memos, including headings, date, recipients, sender's name, and signature fields, etc.

a. Distribution List:

Maintain an up-to-date distribution list for paper memos to ensure that the right individuals receive the information in a timely manner.

b. Tracking and Recording:

Implement a system for tracking and recording the distribution of paper memos, including acknowledgement of receipt and any follow-up actions required.
c. Enforce strict confidentiality measures for sensitive information included in paper memos, such as handling procedures and secure storage.
d. Archiving and Retention: Establish guidelines for the archiving and retention of paper memos, including storage duration and disposal procedures in compliance with data protection regulations.
e. Version Control: Maintain version control for paper memos by including a version number or date to ensure that the most recent information is being referenced.

3. Meeting Etiquette:
    1. Start meetings on time and adhere to the agenda to maximize productivity.
    2. Assign roles (e.g., facilitator, timekeeper) to ensure efficient meeting management.
    3. Encourage active participation and respectful dialogue among team members.

4. Feedback Mechanisms:
    1. Implement regular feedback sessions to gather input on communication effectiveness and areas for improvement.
    2. Provide avenues for anonymous feedback to encourage candid responses.
    3. Act on feedback promptly to address concerns and enhance communication practices.

N. INTERFACING WITH OTHER COMSIT UNITS

Portal and Website Unit:

1. Collaboration on the development and maintenance of the unit's digital presence, including its website, portal, and online platforms for communication and collaboration.
2. Integration of digital innovation initiatives, research projects, and educational resources into the unit's online platforms to enhance visibility and accessibility.
3. Coordination in implementing user-friendly interfaces, intuitive navigation, and responsive design to ensure an optimal user experience for stakeholders.

Training Unit:

1. Partnership in developing and delivering training programs, workshops, and courses on digital innovation, ICT skills, and emerging technologies.

2. Integration of digital innovation and ideation methodologies into training curricula to equip students, faculty, and staff with the knowledge and skills needed for innovation-driven projects.
3. Collaboration on providing hands-on training sessions, experiential learning opportunities, and certification programs to support professional development and lifelong learning.

Helpdesk and Technical Support Unit:

1. Coordination in providing technical support, troubleshooting assistance, and IT solutions to address user inquiries, issues, and service requests related to digital innovation tools and platforms.
2. Collaboration on establishing helpdesk procedures, knowledge bases, and self-service resources to empower users to resolve common issues independently.
3. Integration of helpdesk support channels with the unit's communication channels to ensure seamless access to support services and timely resolution of issues.

Cybersecurity Unit:

1. Partnership in implementing robust cybersecurity measures, policies, and procedures to protect digital innovation projects, research data, and intellectual property from cyber threats.
2. Collaboration on conducting risk assessments, vulnerability scans, and security audits to identify and mitigate security risks in digital innovation initiatives.
3. Coordination in providing cybersecurity training and awareness programs to raise awareness among stakeholders about cyber threats, best practices, and preventive measures.

Network Operating Center (NOC):

1. Collaboration on managing and monitoring the university's network infrastructure, ensuring reliability, performance, and security for digital innovation projects and ICT services.
2. Integration of network monitoring tools, analytics, and dashboards to provide real-time insights into network performance, traffic patterns, and security incidents.
3. Coordination in implementing network upgrades, optimizations, and capacity planning to support the growing demands of digital innovation initiatives and ICT services.

CONCLUSION

In conclusion, the blueprint for a Digital Innovation and ICT Ideation Unit outlines a strategic roadmap for establishing, expanding, and sustaining a dynamic hub for digital innovation, research excellence, and societal impact within the university environment. By following this blueprint, the unit can effectively leverage its resources, expertise, and partnerships to drive innovation, education, and economic development, benefiting both the university community and broader society.

Electronic Learning and Assessment Unit

A. OPERATIONAL BRIEF:

The unit shall be responsible for coordination of digital learning and Assessment process inclusive of the Computer Based Test (CBT) within the University from conception of the idea to its implementation and impact assessment. The unit shall also evaluate the adoption, diffusion and challenges of the newly deployed learning management System.

B. INTRODUCTION

The ELAU Unit is a newly established division within the COMSIT Directorate. The unit will be responsible for implementing, coordinating and evaluating digital learning and impact assessment of Learning Management Systems (LMS) and CBT platforms.

The unit's primary objective is to enhance the efficacy and effectiveness of digital learning and assessment processes, ultimately improving student learning outcomes and academic success.

C. MISSION STATEMENT

The mission of the unit is to plan, design and implement an innovative digital learning and assessment system for the university to enhance student learning experience, outcomes and feedback.

D. STAFFING

1) Head, Electronic Learning and Assessment (ELA): Responsible for developing and implementing electronic learning and digital assessment strategies

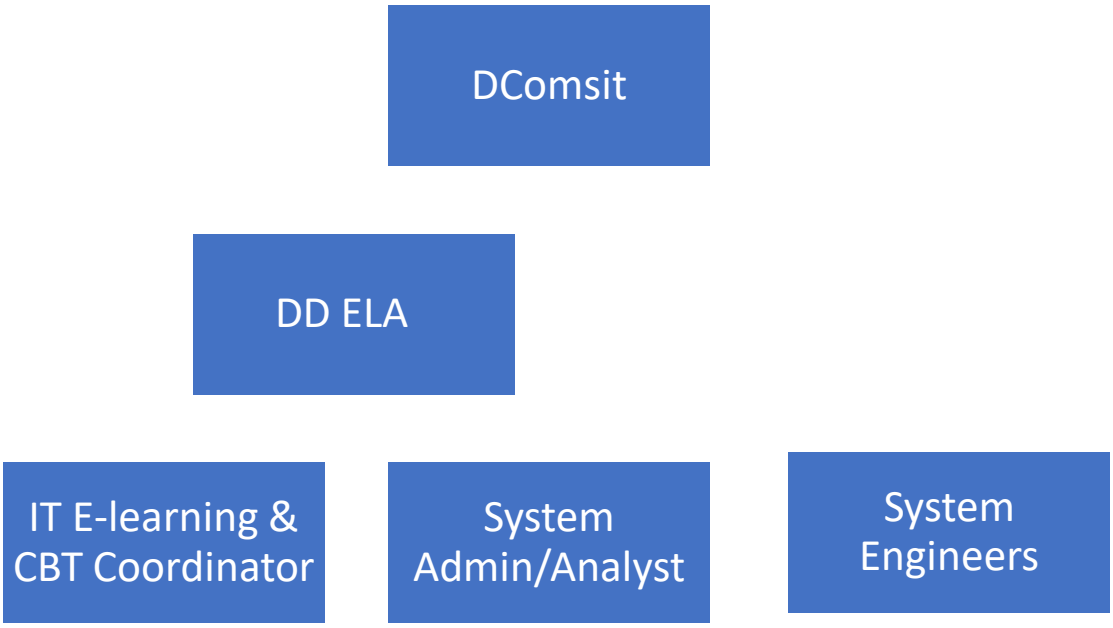
2) Others Staff

1. IT Electronic Learning/Computer Based Assessment coordinator: Responsible for Electronic learning and Computer Based Test implementation, assessment and evaluation

2. IT System Administrator: Provide technical support to students, instructors regarding usage and smooth operation of ELA.

3. System Engineers: hardware repairs failures (e.g server crashes, malfunctioning terminals or broken hardware ELA systems

E. ELA UNIT ORGANOGRAM



F. STRENGTH, WEAK, OPPORTUNITY AND THREAT (SWOT) ANALYSIS

I. Strengths

1. Experienced Staff: Expertise in electronic learning and digital learning and assessment management.

2. Strong Technical Infrastructure: The University has invested heavily in building technical infrastructure to support digital learning activities.

3. Established collaborative relationships with academic departments.

4. Existing Digital Learning Platforms: The University has existing digital learning platforms, such as LMS that can be leveraged to support digital learning initiatives.

5. Flexible and Adaptable Team: The Electronic Learning and Assessment Unit has a flexible and adaptable team that can respond quickly to changing circumstances and priorities.

II. Weaknesses

1. Potential Resistance to Changes: There may be potential resistance to change from Faculty and students who are accustomed to traditional teaching methods.

2. Insufficient Feedback Mechanisms: The Electronic Learning and Assessment Unit's feedback mechanisms may be insufficient, which could impact the success of digital learning initiatives.

Insufficient feedback mechanisms can create risks, such as reduced user adoption, decreased user satisfaction, and increased technical support requests.

3. High Staff Turnover Rate: The Electronic Learning and Assessment Unit may experience a high staff turnover rate, which could impact the unit's ability to maintain continuity and consistency in its service delivery. A high staff turnover rate can create risks, such as reduced institutional knowledge, decreased morale, and increased recruitment and training costs.

III. Opportunities

1. Growing Demand for Online Learning: There is a growing demand for online learning, which presents an opportunity for the Electronic Learning and Assessment Unit to expand its services and to support more students.

2. Increasing Availability of Educational Technology: There is an increasing availability of educational technology, which presents an opportunity for the Electronic Learning and Assessment Unit to leverage on new tools and platforms to support digital learning initiatives.

3. Opportunities for Research and Development: There are opportunities for innovation and development to improve digital learning and assessment systems.

4. Improving Operational Efficiency: There is an opportunity for the Electronic Learning and Assessment Unit to improve its operational efficiency, through training and personal skills development.

IV. Threats

1. Rapidly Changing Technological Landscape: The technological landscape is rapidly changing, which presents a threat to the Electronic Learning and Assessment ability to keep up with the latest technologies and tools.

2. Competition from Other Institutions: There may be an aggressive competition from other institutions, which presents a threat to the Electronic Learning and Assessment Unit's ability to attract and retain students.

3. Potential Data Security and Privacy Concerns: There are potential content and data security concerns, which presents a threat to the Electronic Learning and Assessment Unit's ability to protect and maintain its platform.

4. Limited Institutional Support: There may be limited institutional full support, which presents a threat to the Electronic Learning and Assessment utilizations.

G. KEY PERFORMANCE INDICATORS (KPIs)

1. Unit Head: ELA, system efficiency, user engagement and innovation

KPI : what is the perceived satisfaction by users (students and facilitators) of the digital learning and assessment platform? (usability survey instrument)

2: IT Electronic Learning / Computer Based Coordinator : Measurement of reliability, efficiency and user satisfaction of ELA.

KPI 1: 90 % Digital Learning Platform Adoption Rate: Definition: The percentage of faculty and students using the learning management system (LMS) .

KPI 2: 10% Improvement in student Learning Outcome Improvement: The percentage increase in student learning outcomes as measured by assessments and evaluations.

KPI 3: 95% Faculty Satisfaction with Digital Learning Support

KPI 4: 95% Student Satisfaction with Digital Learning Experience

KPI 5: Technical Support Response Time: 2 hours to response time to technical support requests.

KPI 6: Digital Learning Platform Uptime and Reliability: 24 hours availability and accessibility of learning platforms.

KPI 7: Assessment and Evaluation of content and data meeting quality standards.

KPI 8: 20% Cost savings and efficiency gains

3. System Engineer: CBT of availability and reliability of terminals:

KPI: 95% percentage of computer-based tests (CBT) test administered without technical issues.

H. STANDARD OPERATING PROCEDURES (SOP)

a. Purpose: The Electronic learning and assessment unit is to ensure consistency, efficiency, and quality of service delivery for digital learning materials and assessment tests operations.

b. Responsibilities and Roles

1. Unit Head: Efficiency and innovation of ELA

2. IT Electronic Learning/Computer Based Assessment coordination: Operational reliability, efficiency and user satisfaction of ELA.

3. IT System Administration/Analysis: System uptime, user support and diagnosis tests

4. System Engineers: Time taken to complete hardware repairs or replacements.

c. Reporting Procedure

1. Daily meetings of staff with the Unit Head.
2. Weekly progress reports submitted by each staff to the Unit Head.
3. Monthly reports and reviews with the Director of COMSIT.

d. Escalation Procedure

1. Issue escalated to the Unit Head.
2. Unresolved issues reported to the Director COMSIT

I. LINES OF COMMAND

1. Director of COMSIT
2. Unit Head
3. IT Electronic learning/ Computer Based Test Coordinator
4. System Administrator/Analyst
5. System Engineers

J. DOCUMENT CONTROL

1. Student Assessment Data
2. Quality Assurance and Evaluation Documents
3. Backup and Archival document

K. FUTURE EXPANSION

1. Adoption of new emerging technologies and trends to incorporate innovative features.

2. Skill Development: Invest in training programs to upskill team members and equip them with the latest tools and techniques.

L. COMMUNICATION PLAN

1. Internal Communication:
    1. Regular team meetings to discuss updates, challenges, and achievements.

2. Utilize collaboration tools (e.g. Microsoft Teams) for real-time communication and file sharing.
3. Quarterly unit meetings to share updates and gather feedback from team members.

2. External Communication:

1. Establish a dedicated email address and contact point for external inquiries and feedback.
2. Maintain an active presence on social media platforms to showcase projects, achievements, and job opportunities.
3. Participate in industry events, conferences, and webinars to network and promote the unit's capabilities.

3. International Collaboration:

Foster collaborations with international counterparts to exchange knowledge, best practices, and foster cross-cultural understanding.

M. COMMUNICATION PROTOCOL

1. Email Communication:
    1. Use clear and concise language in email communication.
    2. Include relevant subject lines and action items for quick reference.
    3. Follow up on important emails to ensure timely responses.

2. Hard copy memoranda: Establish a standardized format for hard copy paper memos, including headings, date, recipients, sender's name, and signature fields, etc.

1. Distribution List:
2. Maintain an up-to-date distribution list for paper memos to ensure that the right individuals receive the information in a timely manner.
3. Tracking and Recording:
4. Implement a system for tracking and recording the distribution of paper memos, including acknowledgement of receipt and any follow-up actions required.
5. Enforce strict confidentiality measures for sensitive information included in paper memos, such as handling procedures and secure storage.
6. Archiving and Retention: Establish guidelines for the archiving and retention of paper memos, including storage duration and disposal procedures in compliance with data protection regulations.

e. Version Control: Maintain version control for paper memos by including a version number or date to ensure that the most recent information is being referenced.

3. Meeting Etiquette:

    1. Start meetings on time and adhere to the agenda to maximize productivity.
    2. Assign roles (e.g., facilitator, timekeeper) to ensure efficient meeting management.
    3. Encourage active participation and respectful dialogue among team members.

4. Feedback Mechanisms:

    1. Implement regular feedback sessions to gather input on communication effectiveness and areas for improvement.
    2. Provide avenues for anonymous feedback to encourage candid responses.
    3. Act on feedback promptly to address concerns and enhance communication practices.

N. INTERFACING AREAS WITH OTHER COMSIT UNIT

1. Network Operation Centre(NOC) Unit: To ensure network availability to access assessment of learning management platforms
2. Software and Application Development (unit): Collaborate with this unit for construction and deployment of new features.
3. Digital Innovation and ICT Ideation Unit: Corroborates with this Unit for innovative ways to improve the Unit.
4. Help Desk Unit: Collecting information from this Unit to help gauge Staff and student's responses on the utilization of the system.
5. Training and Development: helps identify, plan and develop training needs for staff and students on electronic learning systems.

O. CONCLUSION

The adoption of electronic learning and assessment technology into the modern educational system represents significant milestones within the university's digital ecosystem. These technologies will facilitate accessibility and flexibility in ELA, allowing students to access learning resources at their own pace.

IT Officers Coordinating Unit

COMPUTER SERVICES AND INFORMATION TECHNOLOGY (COMSIT) DIRECTORATE

A. OPERATIONAL BRIEF

The unit shall see to the efficient delivery of services at Faculties, Centres and Units through effective monitoring of performance of the respective IT Officer. The unit is expected to recommend an outstanding IT Officer for the best IT Officer of the Year award.

The core mandate of an IT Officer includes the following responsibilities:

1. **Technical Support and Maintenance:** Providing technical support to staff, faculty, and students; maintaining and troubleshooting hardware and software issues; ensuring all IT equipment and systems function optimally.

2. **Network Management:** Managing and troubleshooting securing the university's network infrastructure to ensure internet is available

3. **Software and Application Management:** Managing the installation, configuration, and maintenance of base location for ensuring accessibility and compatibility with various devices.

4. **User Training and Support:** Providing training and support to users on various IT systems and tools; developing and delivering instructional materials and workshops.

5. **Collaboration and Communication:** Working closely with other departments and stakeholders to understand their IT needs and provide appropriate solutions; facilitating effective communication within the IT team, base location management.

B. INTRODUCTION

IT Officers are the personnel in charge of deployment and user support of ICT services in various units of the university. The IT Officers provide support and maintenance to computer and network infrastructure to ensure stable operations in the university. They support the Portal Unit and Web services unit in content creation and in solving user needs in Portal related issues. Similarly, they trouble shoot and escalate network down times. They serve as COMSIT Ambassadors in their respective postings.

C. MISSION STATEMENT

To manage and maintain ICT infrastructure and services of faculties, centres and units to ensure efficient, effective and secure operations.

D. STAFFING:

The IT Officers Coordinating Unit renders university-wide ICT services to faculties, centers, and units.

Head of Unit:

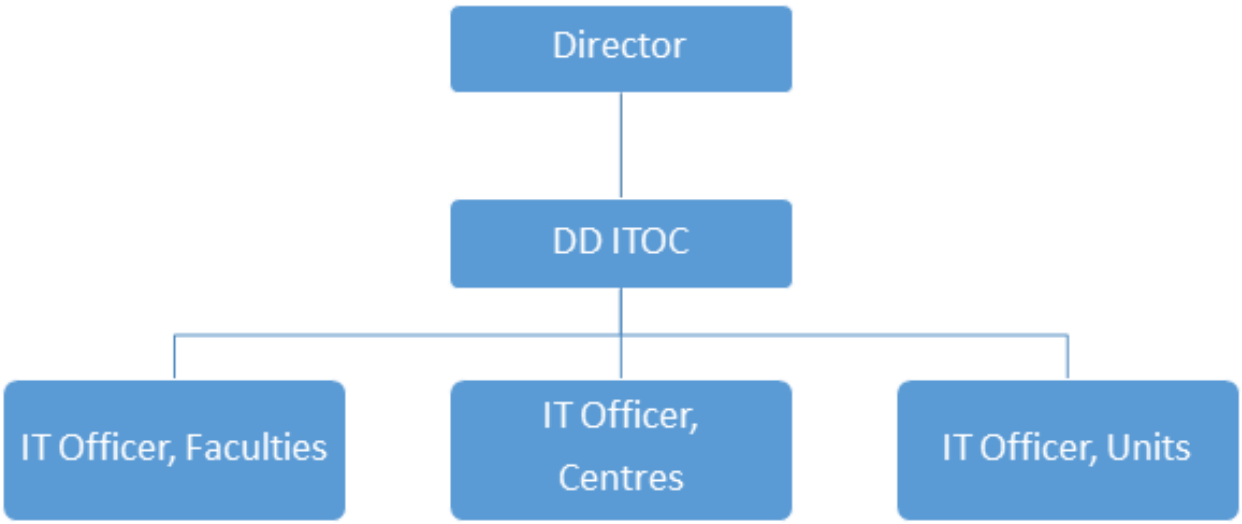
1. Supervising all IT Officers.
2. Interface with faculties, departments, IT Officers and Director COMSIT.
3. In collaboration with Training Unit, organizing programmes for capacity building of IT Officers on ICT innovation for better performance in their operations.
4. Visiting IT Officers in their location base.
5. Reporting issues from faculties to the Director.

IT Officers:

IT Officers' duties are as highlighted below:

1. Assisting students to resolve password issues on both school portal and email.
2. Downloading the students attendance sheet for examinations.
3. Preparing documentation for Faculty board and senate meetings
4. Downloading the students' records or statistics for preparation for clearance and examinations.
5. Organization of trainings and awareness programmes for staff and students on the use of the school portal, and learning management system (LMS).
6. Preparing final year students' data and passport for NYSC mobilization, ID Card and certificate.
7. Resets the students' password and Passport on the undergraduate portal.
8. Designs Google Form to capture students' data for production student ID Card.
9. Troubleshooting of internet downtimes to solve minor internet challenges in the Faculty.
10. Installation of software packages such as operating systems and Office applications.
11. Troubleshooting to solve computer hardware problems including maintenance and repairs.

E. UNIT ORGANOGRAM:



F. SWOT ANALYSIS

Strengths

The key strengths of an IT Officer include:

1. **Technical Expertise:** Proficiency in managing and troubleshooting IT systems, ensuring they run smoothly.
2. **Problem-Solving Skills:** Ability to diagnose and resolve technical issues efficiently.
3. **Communication Skills:** Effective communication with non-technical stakeholders, including faculty, staff, and students.
4. **Adaptability:** Ability to stay updated with the latest technology trends and adapt to changes, and continuously learning and integrating new technologies that benefit the university.
5. **Excellent Service Delivery:** Providing excellent support to the university community.

Ensuring high levels of user satisfaction through timely and effective IT support.

Weakness:

1. Limited Technical Expertise
While IT officers may have strong foundational knowledge, some might lack expertise in more specialized or emerging technologies, such as cloud computing, AI, or advanced cybersecurity protocols. This can limit their ability to effectively manage newer IT systems and infrastructures.
2. Overwhelming Workload
Faculty IT officers often juggle multiple responsibilities, from maintaining hardware and software to providing support for staff and students. This can lead to burnout and a lack of focus on strategic IT planning or innovation, as they are frequently caught up in day-to-day troubleshooting and reactive problem-solving.
3. Lack of Proper Training
Due to limited professional development opportunities or budget constraints, some faculty IT officers may not have access to ongoing training or certification programs. This can result in a knowledge gap, especially as technology evolves rapidly.
4. Communication Gaps
IT officers sometimes struggle to communicate complex technical issues to non-technical faculty members or staff. This can lead to, delays in problem resolution, or underutilization of technology. There may also be a gap in communication between the IT department and faculty, where the latter may not fully express their technology needs or challenges.
5. Limited Budget and Resources
Budgets constraints may restrict the IT officers ability to invest in up-to-date hardware, software, or training.
7. Cybersecurity Vulnerabilities
With increasing reliance on digital platforms, IT officers may face challenges in keeping up with the latest cybersecurity threats and best practices. Without regular updates or comprehensive security training, the institution might be vulnerable to data breaches, phishing attacks, or other cyber threats.

3. OPPORTUNITIES:
An IT Officer in a university typically has a variety of opportunities. This including:

1. Network Management: Overseeing the faculty computer networks, ensuring they run efficiently and securely.
2. Technical Support: Providing assistance to faculty, staff, and students with hardware and software issues.
3. Training and Workshops: Conducting training sessions for staff and students on new technologies and best practices in IT.
4. IT Policy Development: Helping to develop and enforce IT policies and procedures within the university.

4. Threat :

The main threats and challenges faced by an IT Officer at a university typically include:

1. **Cybersecurity Threats:** Challenge: Protecting the university's data and systems from cyber attacks, such as phishing, ransomware, and hacking. Example: Regularly updating security protocols and educating the university community on cybersecurity best practices.

2. **Data Breaches:** Challenge: Preventing unauthorized access to sensitive information, including student records, research data, and financial information. Example: Implementing strong access controls and encryption methods.

Technology Obsolescence: For compatibility with emerging technologies, all ICT equipment must be recent and trending. Keeping up with rapid technological changes and ensuring the university's IT systems remain current.

G. KEY PERFORMANCE INDICATORS (KPIS)

Key Performance Indicators (KPIs) for IT Officers help measure their effectiveness and efficiency in managing the ICT services and infrastructure.

1. **Technical Support and Help-desk Performance:** User Satisfaction Score: Feedback rating from users on the quality of support received through the standard e-ticketing facility.

2. **Software and Application Management:** User Adoption Rate: Percentage of target users actively using new software.

Issue Resolution Time: Average time taken to resolve application-related issues.

3. **User Training and Support:** Training Session Attendance: Number of users attending IT training sessions.

4. **Innovation and Improvement:**

New Technology Implementations: Number of new technologies successfully deployed.

Process Improvement Initiatives: Number of initiatives to improve IT processes and efficiency.

H. Standard Operating Procedure:

The standard operating procedures (SOPs) for IT Officers involve a range of responsibilities to ensure the smooth operation and security of the institution's IT infrastructure. The following are common tasks and responsibilities:

1. Providing technical support to students, faculty, and staff, including troubleshooting hardware and software issues.
2. Offering training sessions or creating guides for users on various IT systems and software used at the university.
3. Installing and updating software on university computers.
4. Producing hard-copy documentation of various student details from the university porta

I. LINE OF COMMAND

Director, COMSIT
Deputy Director/Head of the unit
Faculty/Centre/Unit IT Officer

L. DOCUMENTATION CONTROL

Types of Documents:

Requests document
Completed request document
Version Control System:
Document Approval Process:
Access Control
Document Storage and Retrieval

M. COMMUNICATION PLAN

The communication between the unit (ITOC), COMSIT, Faculty and entire university is via : paper trail, electronic mail, phone call, person to person and internet-enabled calls.

N. INTERFACING AREAS WITH OTHER COMSIT UNITS

The IT Officer interfaces with various units within the university to ensure seamless IT operations, support academic and administrative functions, and enhance overall productivity. Here are the general primary areas of interaction:

1. Academic Departments:

Faculty and Staff Support: Provide technical support for teaching and research activities.
Classroom Technology: Maintain and support audio-visual equipment and other classroom technologies.

2. Administrative Units

Human Resources: Assist with onboarding and off boarding processes, ensuring access to IT systems and resources.

Registrar's Office: Manage student information systems and provide support for enrollment, grading, and scheduling software.

3. Student Services:

Help-desk Support: Provide technical assistance to students for accessing university systems and resources.

Online Learning Platforms: Support and maintain learning management systems (LMS) and other e-learning tools.

Campus Services: Assist with IT needs related to campus housing, health services, and student organizations.

O. CONCLUSION

It is clear that effective IT Officers are pivotal in shaping the future of education. Ultimately, this write-up serves as a call to action for our university to invest in and prioritize her IT infrastructure and personnel, ensuring they remain at the forefront of innovation.

Mail Services and Help Desk Unit

COMPUTER SERVICES AND INFORMATION TECHNOLOGY (COMSIT) DIRECTORATE

A. OPERATIONAL BRIEF

The unit shall be responsible for general mail services for students and staff of the University including managing the mail server in a very secure manner based on global best practices. The unit shall equally coordinate technical support services through the new e ticketing and supports email platforms to address all forms of user's challenges within reasonable time

B INTRODUCTION

The Mail Services and Help Desk Unit (MSH) is an important arm of the Computer Services and Information Technology (COMSIT) Directorate at the University of Ilorin. The unit is responsible for administering and managing mail server/email services, including creating and maintaining email addresses for the university community. It also handles the help desk operations, providing quick responses to information delivery and technical support issues. The unit aims to improve service delivery continuously, optimizing email usage for information dissemination and knowledge sharing while ensuring high standards of webmail and helpdesk services**.**

C. MISSION STATEMENT

1. **Mission:** To deliver exceptional email and help desk services that support the university's academic, administrative functions through reliable, secure, innovative solutions, fostering seamless communication, enhanced user experience.

D. STAFFING:

Job Description: Mail Server and Help Desk Team.

1. **Head of Unit(1):** Managing and overseeing the operations of the unit.
2. **Mail Server Administrator(1):** This staff is responsible for managing and maintaining the University's email infrastructure. Primary goal is to ensure reliable, secure, and efficient email services.

Key responsibilities:

. **Server management:** Installing, configuring, and upgrading mail servers, including hardware and software maintenance.

I. **Email account management:** Creating, modifying, and deleting email accounts, as well as managing access controls and permissions.

II. **Security and spam management:** Implementing and maintaining security measures to prevent spam, viruses, and other email-borne threats.

III. **Performance monitoring and optimization:** Monitoring email server performance, identifying bottlenecks, and optimizing system resources for improved efficiency.
IV. **Troubleshooting:** Resolving email-related issues, such as delivery problems, authentication errors, and client configuration issues.
V. **Compliance and policy management:** Ensuring email services comply with organizational policies, regulatory requirements, and industry standards.
VI. **Backup and recovery:** Implementing backup and recovery procedures to ensure business continuity in case of email server failures or data loss.
VII. **Documentation and reporting:** Maintaining accurate documentation and generating reports on email server performance, usage, and security incidents.

3.System Analyst(2): The System Analyst here plays a crucial role in bridging the gap between university community needs as Related to emailing and technology solutions. They analyze and design mail server systems to improve efficiency, productivity, and overall performance.

Key Responsibilities:

. **System Design:** Designing and proposing mailing system solutions to meet needs, including hardware, software, and infrastructure requirements.

II. **System Integration:** Integrating new mailing systems with existing infrastructure, ensuring seamless communication flow and minimal disruption. Conducting thorough testing to ensure mailing systems meet requirements and are free from defects.

III. **Implementation and Deployment:** Overseeing the implementation and deployment email addresses to the University community and deployment of new systems, providing training and support to end-users.
IV. **Maintenance and Troubleshooting:** Performing routine maintenance, troubleshooting issues, and applying patches and updates to ensure system stability

4. **Help Desk Officer :** A Help Desk Officer, also known as a Technical Support Specialist or Service Desk Technician, is responsible for providing assistance and support to the university communities with technical issues or product-related questions.

Key Responsibilities:

. Responding to users' inquiries via phone, email, chat, or in-person.
I. Troubleshooting and resolving technical issues with hardware, software, or networks.
II. Providing product information, guidance, and training to users.
III. Documenting users interactions, issues, and resolutions in an e-ticketing system.
IV. Escalating complex issues to higher-level support teams or specialists.

V. Participating in knowledge-sharing activities to improve team performance and stay up-to-date with new technologies.

5. **ICT support Staff (1):** ICT Information and Communications Technology) Support Staff, also known as IT Support or Technical Support, play a vital role in ensuring the smooth operation of an organization's technology infrastructure.

Key Responsibilities:

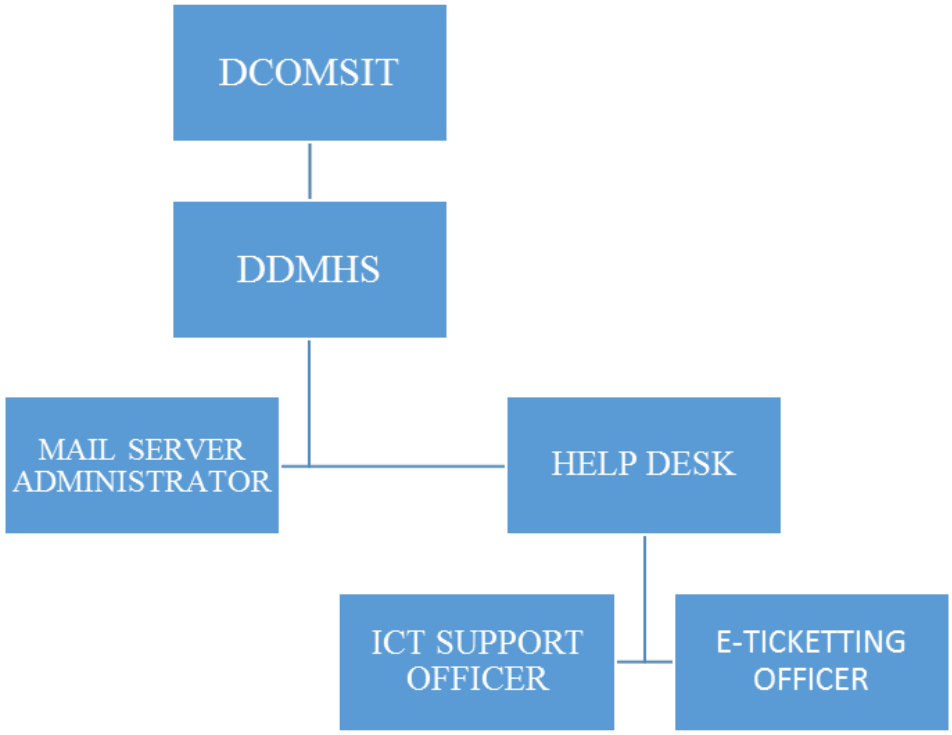
I. **Troubleshooting:** Identifying and resolving hardware, software, and network issues.
II. **Technical Assistance:** Providing support and guidance to users via email, phone or in-person.
III. **Maintenance and Repair:** Performing routine maintenance, repairs, and upgrades to hardware and software.
IV. **Installation and Configuration:** Installing, configuring, and testing new hardware and software.
V. **Network Administration:** Managing and maintaining network infrastructure, including routers, switches, and firewalls.
VI. **Security:** Ensuring the security and integrity of the organization's data and systems.
VII. **Documentation:** Maintaining accurate records of technical issues, resolutions, and system configurations.

6. **E-ticketing officer:** An e-Ticketing Officer is responsible for managing and resolving users support requests and issues through an electronic ticketing system. Their primary goal is to provide timely and effective support to users, ensuring their issues are resolved efficiently.

Key Responsibilities:

. **Managing e-Ticketing System:** Creating, assigning, and tracking e-tickets to ensure timely resolution of user issues.
I. **Users Support:** Responding to users inquiries, resolving issues, and providing product or service information via email, phone or chat.
II. **Issue Resolution:** Troubleshooting and resolving technical issues, escalating complex problems to senior support staff or specialists when necessary.
III. **Ticket Management:** Updating ticket status, categorizing issues, and ensuring accurate documentation of users interactions.
IV. **Reporting and Analytics**: Generating reports on ticket volume, resolution rates, and users satisfaction to identify trends and areas for improvement.
V. **Process Improvement:** Suggesting and implementing process enhancements to improve efficiency, users satisfaction, and first-call resolution rates.

E. UNIT ORGANOGRAM



F SWOT ANALYSIS

1. Strengths:

. **Free and Easy to Use:** Email services are made available to members of the university at no cost.

I. **Quick Communication:** Fast and efficient information dissemination.

II. **Global Reach:** Email is accessible worldwide, facilitating global communication.

III. **Supportive Infrastructure:** Strong administrative support and user-friendly helpdesk services.

2. Weaknesses:

. **Email Literacy:** Some staff and students struggle with using their email addresses effectively.
I. **Password Issues:** Frequent issues with forgotten login IDs and passwords.
II. **Service Dependency:** Heavy reliance on Google for webmail services.

3. Opportunities:

. **Collaboration with Google:** Strengthening relationships with Google to enhance service delivery.
I. **Google Workspace for Education:** Leveraging Google Classroom and Google Meet for academic and administrative support.
II. **User Training:** Providing comprehensive training programs to improve email and help-desk usage.

4. Threats:

. **Phishing Attacks:** Risk of phishing emails compromising user credentials and data.
I. **Suspicious Logins:** Vulnerability to unauthorized access and data breaches.
II. **Leaked Passwords:** Potential for compromised passwords leading to unauthorized access.
III. Deactivation of emails of staff who are no longer active in the system.

G. KEY PERFORMANCE INDICATORS (KPIs)

1. **Email Server Uptime:** Measuring the uptime of mail server with a benchmark of 99.9% over a period of time.
2. **Help-desk Response Time:** Measure the average response time against a benchmark of 1 hour over a period of time.
3. **Users Satisfaction:** Measuring user satisfaction against a benchmark of 90% over a period of time.
4. **Email Delivery Success Rate:** Measure the percentage of undelivered email with a benchmark of >= 2%.
5. **Spam Detection Rates:** Achieve a spam and malware detection rate of 99% or higher.
6. **User Training Sessions:** Conduct at least 12 user training sessions annually.
7. **Password Reset Efficiency:** Resolve 95% of password reset requests within 24 hours.
8. **Security Incident Mitigation:** Mitigate 100% of reported security incidents within defined SLA times.
9. **Phishing Awareness Training:** Provide phishing awareness training to 100% of staff and students annually.
10. **Service Enhancement Implementation:** Implement at least 5 significant service enhancements annually based on user feedback.

H. STANDARD OPERATING PROCEDURE (SOP) PURPOSE: This SOP provides guidelines for the Mail Services and Helpdesk Unit operations to ensure efficient, secured, world-class services to the University of Ilorin community.

SCOPE

This SOP applies to all activities related to managing and maintaining email services and helpdesk support within the University of Ilorin.

PROCEDURES

EMAIL SERVICES:

1. **Account Management:**
    1. Create and manage email accounts using the Mail Server Admin Console.
    2. Reset passwords and assist with login issues.

    Security Measures:
    - Implement multi-factor authentication and encryption protocols.
    - Monitor for phishing attacks and unauthorized access.
1. **Service Availability:**
    i. Ensure high availability and performance of email services.
    ii. Conduct regular maintenance and updates.

User Training:
i. Provide training on email usage and security best practices.
ii. Conduct phishing awareness sessions.

HELPDESK SUPPORT

1. **Resolution of Issues:**
    i. Use of the university e-ticketing system to manage and resolve user escalated complaints and queries.
    ii. Prioritize and escalate issues to the appropriate level as necessary.

Users Service:
i. Maintain a professional and helpful attitude.
ii. Ensure quick and efficient resolution of support requests.

Performance Monitoring:
i. Track response and resolution times.
ii. Collect feedback from users to improve services.

I. Lines of Command (top-down)

1. Director of COMSIT
2. Unit Head

3. Project Manager
4. Team Leads (Business Analyst, System Administrator, etc.)
5. Individual Contributors (Developers, QA Engineers, etc.)

J. Document control

Types of Documents:

1. Requirements Specifications
2. Design Documents
3. Test Plans and Reports
4. User Manuals
5. Change Requests

K. FUTURE EXPANSION PLANS

1. **Infrastructure Assessment:** Evaluate current mail server infrastructure for improvements.
2. **Scalability Planning:** Design scalable solutions for future growth.
3. **Security Enhancements:** Implement advanced threat detection and regular security audits.
4. **High Availability and Disaster Recovery:** Design architectures for continuous access and establish recovery plans.
5. **Automation and Monitoring:** Implement tools for routine tasks and continuous monitoring.
6. **User Training and Support:** Provide resources and dedicated support channels for users.

L. COMMUNICATION PLAN

1. **Email Newsletters**: Send regular updates and essential information to all stakeholders.
2. **Intranet Portal**: Maintain a section with FAQs, troubleshooting guides, and announcements.
3. **Social Media**: Use official university accounts for broader announcements and updates.
4. **Meetings and Workshops**: Conduct periodic sessions to address concerns, provide training, and gather feedback.
5. **Surveys:** Collect feedback and suggestions for continuous improvement.

M. COMMUNICATION PROTOCOL: In a mail server service, the line of communication refers to the flow of information between different components, systems, or individuals. Here's a breakdown of the typical lines of communication:

. **Internal Communication:**

1. Mail Server-Database: The mail server interacts with
2. a database to store and retrieve email data, user accounts, and settings.
3. Mail Server-Antivirus/Anti-spam: The mail server
4. communicates with antivirus and anti-spam systems to scan emails for malware and spam.
5. Mail Server-Authentication System (2-step): The mail
6. server interacts with an authentication system (e.g., LDAP, Active Directory) to verify user credentials.

II. External Communication:

1. User-Mail Server: Users send and receive emails
   through the mail server using email clients (e.g., Gmail, Outlook).
   ail Server-Internet: The mail server communicates
2. with other mail servers on the internet to send and receive emails.

These lines of communication work together to enable the mail server service to manage email transmission, reception, and storage.

N. INTERFACING AREAS WITH OTHER COMSIT UNITS.

1. Cross-Unit Collaboration:

- Regular meetings with representatives from each unit.
- Share knowledge and resources to improve service delivery.

Joint Projects: Identify and execute joint projects that leverage multiple units' expertise.

O. CONCLUSION:

The Mail Services and Help-desk Unit supports the University of Ilorin's ICT infrastructure through deployment of efficient email and help-desk services. By addressing its strengths, weaknesses, opportunities, and threats and focusing on key performance indicators, the unit strives to achieve its mission and vision. Continuous improvement and user-focused initiatives will ensure the unit remains a cornerstone of effective communication and technical support within the university, contributing significantly to its reputation as a leading higher education institution in Nigeria and beyond.

Network Operations Unit

A. OPERATIONAL BRIEF

The unit is responsible for the smooth running of the University's Network Operations Centre (NOC) in ensuring seamless planning, deployment and maintenance of bandwidth, network, green energy and other digital infrastructure across the University. The unit is to come up with standard operation procedures capable of achieving sustainable digital transformation given efficient digital infrastructures.

B. INTRODUCTION

This blueprint establishes a strategic framework and Standard Operating Procedures (SOPs) for the University of Ilorin's Network Operations Center (NOC). It aims to enhance operational excellence and align with global best practices of world-class universities.

The NOC functions as the university's network services core, providing campus-wide connectivity and external campuses. The current infrastructure uses a core-distribution-access model, with fifteen network distributions connecting buildings at access levels.

This document outlines key NOC operational mandates:

1. Network Infrastructure Management
2. Network Security and Monitoring
3. Server and Data Management
4. Help Desk and Support
5. Power and Cooling Administration

C. MISSION STATEMENT

The unit aims to provide seamless network operations, proactively manage and maintain the campus-wide digital infrastructure(Green Energy), and provide ICT support.

D. STAFFING

Head of Unit (1): provide strategic direction and oversee all operations of NOC.

A. Network Infrastructure Management

1. **Network Administrator (1):** Designs, implements, and maintains the overall network architecture. Develops long-term plans for network expansion and upgrades. Ensures interoperability of all network systems. Collaborates with other sub-units of NOC.
2. **Senior Network Engineers (2):** Responsible for the design, implementation, and maintenance of specific network segments (e.g., fiber optics, LAN, wireless). Troubleshoots complex network issues. Provides technical expertise and guidance to junior engineers.

3. **Network Engineers (2):** Implement and maintain network infrastructure according to designs. Perform routine maintenance and troubleshooting. Monitor network performance. Assist Senior Network Engineers.
4. **Network Technicians (4):** Install and maintain physical network infrastructure (cabling, equipment). Perform basic troubleshooting and maintenance. Assist engineers with larger projects.

B. Network Security & Monitoring

1. **Network Security Engineer (1):** Develops and implements network security policies and procedures. Manages firewalls, intrusion detection/prevention systems, and other security tools. Conducts security audits and vulnerability assessments. Responds to security incidents.
2. **Network Security Analyst (1):** Monitors network traffic for suspicious activity and security breaches. Analyzes security logs and reports. Collaborates with Security Engineer on incident response.
3. **Network Monitoring Specialist (1):** Monitors network performance using NMS. Sets up and configures monitoring tools. Analyzes monitoring data and creates reports. Responds to alerts, performs initial troubleshooting.

C. Server & Data Management

System Administrator (2): Manage and maintain servers, including operating systems, applications, and databases. Perform regular maintenance tasks (updates, backups). Ensure server security. Implement and monitor access control policies. Resolve server-related incidents.

1. **Database Administrator (1):** Manage and maintain databases, ensuring data integrity and availability. Perform regular backups and implement recovery procedures. Optimize database performance.
2. **Data Center Technician (1):** Responsible for the physical maintenance of the server room, including power and cooling systems. Monitors environmental conditions and responds to alerts.

D. Help Desk & Support

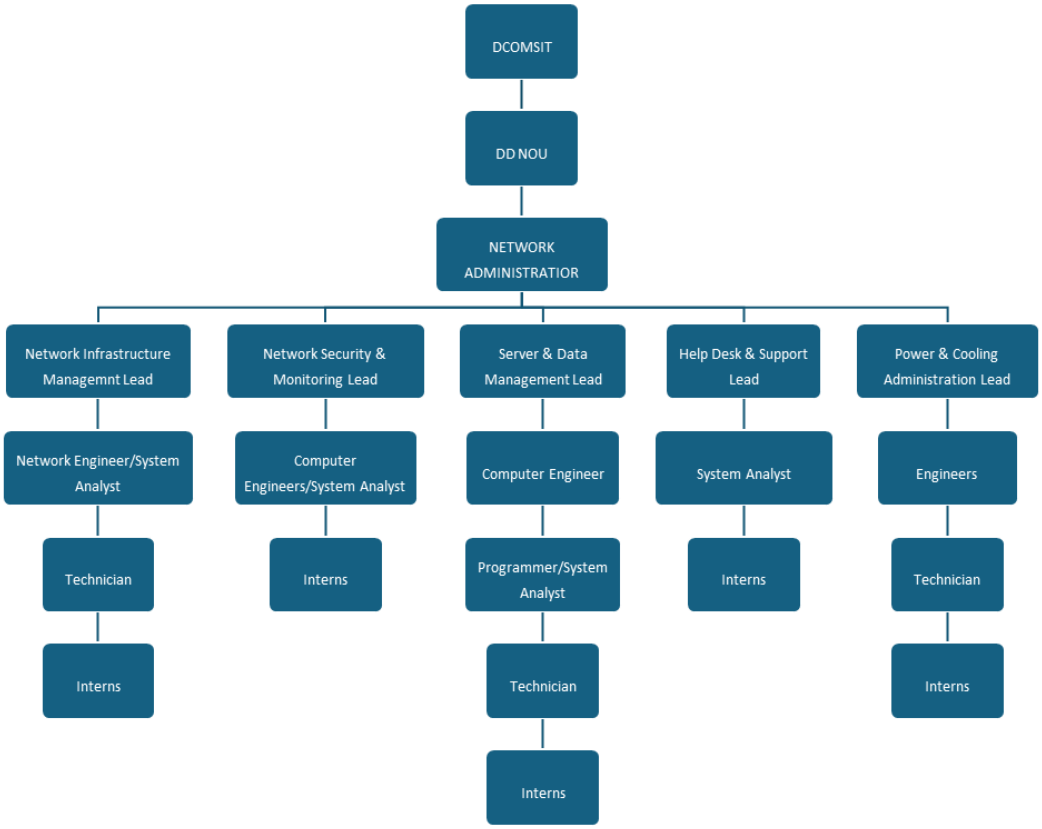
1. **Help Desk Manager (1):** Oversees Help Desk operations, ensuring SOP compliance and efficient handling of all network-related queries and issues. Manages staff, develops training programs, and creates reports.
2. **Help Desk Analysts (2):** Provide first-level support to end-users, troubleshooting common issues, and escalating complex issues to second-level support. Create and manage tickets within the IT service management (ITSM) system.

3. **Second-Level Support (2):** Provide in-depth troubleshooting and technical support for complex network issues. Collaborate with other IT units as needed.

E. Power and Cooling Administration

1. **Power & Cooling Engineer (1):** Responsible for designing, implementing, and maintaining power and cooling systems within the NOC and other distributions across the campus. Develops and implements preventative maintenance plans. Responds to power and cooling system alerts and performs troubleshooting. Monitors environmental conditions.
2. **Power & Cooling Technician (1):** Performs routine maintenance on power and cooling equipment. Assists the engineer with more complex tasks.

E. UNIT ORGANOGRAM:



F. SWOT ANALYSIS

The SWOT analysis provides a clear picture of the current state of the NOC and outlines opportunities for improvement. Addressing the weaknesses and capitalizing on the opportunities while mitigating the threats will allow the University of Ilorin NOC to realize its strategic goals of technological excellence and operational resilience.

A. Strengths:

1. **Centralized Management:** The NOC's centralized structure facilitates efficient oversight and management of the entire campus network, ensuring consistency and coordination across various units and locations.
2. **Comprehensive Infrastructure:** The existing fiber-optic and wireless infrastructure provides a solid foundation for robust connectivity, although expansion and upgrades are needed. The shift towards a fiber-optic backbone is a significant step forward.
3. **Proactive Maintenance:** The emphasis on proactive maintenance, regular inspections, and preventive measures demonstrates a commitment to minimizing disruptions and maximizing uptime. The integration of renewable energy sources through a Cluster-Based-Solar Inverter system is also a significant strength.
4. **Security Focus:** The inclusion of comprehensive security measures, including regular audits, intrusion detection/prevention systems, and incident response plans, demonstrates a strong commitment to network security.
5. **Comprehensive SOPs:** Detailed SOPs for various NOC functions provide clear guidelines for operations, ensuring consistency and efficiency.

   Dedicated Staff: The existing staff members show dedication and experience in managing and maintaining the network, although additional personnel are needed to fully support the comprehensive strategy.

B. Weaknesses:

1. **Fiber-Optic Connectivity Gaps:** While significant progress is being made, a substantial portion of campus buildings lack direct fiber-optic connections, potentially hindering network performance and scalability.
2. **Wireless Coverage Shortfalls:** The existing wireless infrastructure falls short of meeting the estimated requirements, impacting coverage and potentially affecting connectivity, especially in dense areas.
3. **Power Backup Limitations:** While an innovative power strategy is in place, a significant portion of the power clusters remain inactive, leaving the network vulnerable to power outages.
4. **Maintenance Backlog:** The presence of a maintenance backlog indicates a need for improved resource allocation to address outstanding network maintenance issues promptly.
5. **Staffing Shortages:** The existing staff are inadequate and additional staff across all departments are required to maintain operational excellence and support the comprehensive plan.
6. **Data Center Limitations:** The transition to licensed virtualization and the implementation of high-level firewalls remains incomplete.

C. Opportunities:

1. **Fiber-Optic Expansion:** The University's ICT policy for full fiber-optic connectivity presents a prime opportunity to significantly enhance network reliability, scalability, and future-proofing.
2. **Wireless Network Enhancement:** Addressing wireless coverage gaps by deploying additional enterprise-grade wireless radios will improve user experience and campus-wide connectivity
3. **Technological Advancements:** Embracing Software Defined Networking (SDN), network virtualization, and other innovative technologies can significantly improve network performance and management efficiency.
4. **Renewable Energy Integration:** Further development of the Cluster-Based-Solar Inverter system will reduce dependency on the national grid, leading to improved cost-efficiency and sustainability.
5. **Improved Monitoring and Security:** Implementing advanced monitoring and security tools and systems will enhance proactive threat detection, minimize downtime, and strengthen the NOC's security posture.
6. **Stakeholder Collaboration:** Establishing effective communication channels and strong working relationships with stakeholders will support network development and meet the evolving needs of the university community.
7. **Staff Development:** Investment in training and certification will enhance the skills and expertise of NOC staff, ensuring the team remains at the forefront of technological advancements.

D. Threats:

1. **Budgetary Constraints:** Limited funding could hinder the implementation of strategic initiatives and necessary expansions. Innovative funding strategies are crucial.
2. **Cybersecurity Threats:** The university's network is constantly vulnerable to cyber threats, requiring ongoing vigilance, security audits, and prompt incident response mechanisms.
3. **Power Instability:** The NOC's reliance on the national grid, while being augmented by renewable sources, leaves it susceptible to power outages, highlighting the importance of robust backup power systems.
4. **Technological Obsolescence:** Keeping abreast of rapidly changing technology and regularly updating hardware and software is essential to maintain network performance and security.
5. **Regulatory Non-Compliance:** Failure to adhere to relevant policies and regulations could result in legal and reputational risks.

G. KEY PERFORMANCE INDICATORS (KPIs)

The Key Performance Indicators (KPIs) for evaluating staff and job descriptions within the NOC blueprint for the University of Ilorin, are categorized by the five core mandates. These KPIs are designed to be measurable, relevant, and aligned with best practices in higher education IT system.

A. Network Infrastructure Management:

1. **Fiber Optic Network Uptime:** Percentage of time the fiber optic network is operational. Target: 99.99%
2. **LAN/Wireless Network Uptime:** Percentage of time the LAN and wireless networks are operational. Target: 99.95%
3. **Mean Time To Repair (MTTR) for Network Outages:** Average time taken to resolve network outages. Target: Under 1 hour for critical outages, under 4 hours for non-critical outages
4. **Successful Infrastructure Project Completion Rate:** Percentage of planned network infrastructure projects (upgrades, installations) completed on time and within budget. Target: 95%
5. **Network Infrastructure Documentation Accuracy:** Percentage of network devices and infrastructure accurately documented in the network inventory. Target: 100%

B. Network Security & Monitoring:

1. **Security Incident Response Time:** Average time taken to respond to and resolve security incidents. Target: Under 30 minutes for critical incidents, under 2 hours for non-critical incidents
2. **Number of Security Vulnerabilities Detected and Remediated:** Tracks the number of vulnerabilities identified through regular scans and the percentage successfully remediated within the defined timeframe. Target: 100% remediation within 72 hours of detection.
3. **Network Uptime as a Result of Proactive Monitoring:** Percentage of network downtime prevented through proactive monitoring and timely intervention. Target: 98%
4. **Accuracy of Security Audits:** Percentage of security audits completed accurately and within the given timeframe. Target: 100%
5. **False Positive Rate in Security Monitoring Systems:** Percentage of alerts generated by security monitoring systems that are false positives. Target: Below 10%

C. Server & Data Management:

1. **Server Uptime:** Percentage of time servers are operational. Target: 99.9%

2. **Successful Backup Completion Rate:** Percentage of server backups completed successfully. Target: 100%
3. **Average Time to Restore Server Services After an Outage:** Average time to restore server services after an outage. Target: Under 30 minutes for critical services.
4. **Data Loss Rate:** Tracks instances of data loss due to server failure or other incidents. Target: 0% data loss
5. **Compliance with Data Backup and Retention Policies:** Tracks adherence to data retention and backup procedures. Target: 100%

D. Help Desk & Support

1. **Average Ticket Resolution Time:** Average time taken to resolve Help Desk tickets. Target: Under 2 hours for high priority, under 4 hours for normal priority. Perc
2. **User Satisfaction Rate:** Percentage of users satisfied with Help Desk services, measured through surveys. Target: 90%
3. **First Call Resolution Rate:** Percentage of Help Desk tickets resolved on the first contact. Target: 70%
4. **Number of Escalated Tickets:** Number of tickets that were escalated to second-level support. Target: Below 15%
5. **Help Desk Ticket Resolution Accuracy:** Percentage of Help Desk tickets resolved correctly on the first attempt. Target: 98%

E. Power & Cooling Administration:

1. **NOC Uptime due to Reliable Power:** Percentage of NOC downtime caused by power outages. Target: 0%
2. **UPS System Availability:** Percentage of time the UPS system provides uninterrupted power. Target: 100%
3. **HVAC System Uptime:** Percentage of time the HVAC system maintains optimal environmental conditions. Target: 99%
4. **Mean Time To Repair (MTTR) for Power/Cooling Outages:** Average time taken to resolve power or cooling system outages. Target: Under 1 hour for critical events.
5. **Adherence to Preventive Maintenance Schedule:** Percentage of preventive maintenance tasks completed according to schedule. Target: 100%

H. STANDARD OPERATING PROCEDURE (SOP)

STANDARD OPERATING PROCEDURE FOR NETWORK INFRASTRUCTURE MANAGEMENT SUB UNIT

1. Purpose: This SOP establishes the processes and procedures for effective management and maintenance of the University's network infrastructure, ensuring high availability, performance, security, and compliance with University policies and industry best practices. This SOP directly supports the strategic goals of the NOC under COMSIT Directorate.

2. Scope: This SOP encompasses all aspects of network infrastructure management, including:

. **Network Planning and Design:** Future-proofing the network, including capacity planning, technology selection, and architectural design for scalability and resilience.

I. **Implementation and Deployment:** Physical installation, configuration, testing, and documentation of all network devices and infrastructure.

II. **Maintenance and Operations:** Proactive and reactive maintenance, including troubleshooting, upgrades, and performance monitoring.

III. **Documentation and Inventory:** Maintaining accurate and up-to-date network documentation, diagrams, and inventory records.

IV. **Security:** Implementing and enforcing network security policies and procedures.

V. **Vendor Management:** Managing relationships with network vendors and service providers.

3. Roles and Responsibilities: (Note: The number of personnel in each role will be determined by the size and complexity of the network infrastructure.)

. **Network Infrastructure Management Lead:** Overall responsibility for the network infrastructure management sub-unit. Develops and implements strategic plans, manages staff, and reports to the Network Administrator.

I. **Network Architect:** Designs, implements, and maintains the overall network architecture. Develops long-term plans for expansion and upgrades, ensuring interoperability and compliance with industry standards.

II. **Senior Network Engineers:** Responsible for design, implementation, and maintenance of complex network segments (e.g., fiber optics, core routing). Provide advanced troubleshooting and technical guidance to junior engineers.
III. **Network Engineers:** Implement and maintain network infrastructure according to designs. Perform routine maintenance, troubleshooting, and performance monitoring.
IV. **Network Technicians:** Install and maintain physical network infrastructure (cabling, equipment). Perform basic troubleshooting and maintenance; assist engineers with larger projects.
V. **Data Center Technician:** Responsible for the physical maintenance of the server rooms and network closets, including power and cooling systems.

4. Line of Command and Reporting:

. All Network Infrastructure Management staff report to the Network Infrastructure Management Lead.
I. The Network Infrastructure Management Lead reports to the Network Administrator.
II. The Network Administrator reports to the Head of the NOC.
III. The Head of the NOC reports to the Director, COMSIT.

5. Processes and Procedures:

. **Change Management:** All changes to the network infrastructure (hardware, software, configuration) must follow a change management procedure.
I. **Incident Management:** A well-defined incident management process is in place, including clear escalation paths, communication protocols, and reporting procedures.
II. **Problem Management:** Proactive identification and resolution of recurring network problems to prevent future incidents.
III. **Preventive Maintenance Schedule:** A detailed preventative maintenance schedule is developed and implemented, covering all network devices and infrastructure.
IV. **Capacity Planning:** Regular capacity planning should be conducted to ensure continuous service improvement for current and future demands.

V. **Network Security Policy:** University network security policy and infrastructure management activities must adhere to University network security policies and procedures. Regular network security audits should be conducted.

VI. **Vendor Management:** Relationships with network vendors are managed through contracts, service level agreements (SLAs), and regular communication.

VII. **Documentation:** Comprehensive network documentation is maintained, including diagrams, configurations, inventory records, and standard operating procedures.

6. Escalation Matrix:

Issue Type	Level 1 (Technician)	Level 2 (Engineer)	Level 3 (Lead/Architect)
Minor network issues	Troubleshoot and resolve	Escalate if unresolved	Review resolution
Major network outages	Escalate immediately	Troubleshoot and escalate	Coordinate resolution
Security incidents	Escalate immediately	Investigate and escalate	Manage response
Capacity issues	Report to Lead	Analyze and recommend	Plan and implement

7. Performance Measurement: KPIs (Key Performance Indicators) are used to monitor the effectiveness of the Network Infrastructure Management sub-unit:

. **Network Uptime (Fiber & Wireless):** Targets should be set based on industry best practices and service level agreements (e.g., 99.99% for fiber)over a period of time.

I. **Mean Time To Repair (MTTR):** Defined targets for resolving network outages based on severity (e.g., under 1 hour for critical outages).

II. **Successful Project Completion Rate:** Track percentage of network projects completed on time and within budget.

III. **Documentation Accuracy:** Maintain 100% accuracy of network documentation.

IV. **Security Incident Response Time:** Targets for resolving security incidents based on severity.

7. Review and Updates: This SOP must have review due date(RDD) and should have strictly adhered to,so as to reflect technological advancements, changes to the network infrastructure, and evolving organizational requirements.

STANDARD OPERATING PROCEDURE (SOP) FOR NETWORK SECURITY AND MONITORING SUB UNIT

1. Purpose: This SOP defines the processes and procedures for securing and monitoring the University's network infrastructure to ensure its confidentiality, integrity, and availability. It supports the overall strategic goals of the NOC and COMSIT.

2. Scope: This SOP covers all aspects of network security and monitoring, including:

1. **Security Policy Enforcement:** Implementing and enforcing network security policies and procedures.
2. **Threat Detection and Prevention:** Deploying and managing security tools to detect and prevent security threats.
3. **Security Monitoring:** Continuous monitoring of network activity for suspicious behavior.
4. **Incident Response:** Handling security incidents according to established procedures.
5. **Vulnerability Management:** Identifying and remediating network vulnerabilities.
6. **Security Awareness Training:** Educating users about network security best practices.
7. **Security Auditing:** Regularly auditing network security controls.

3. Roles and Responsibilities:

1. **Network Security and Monitoring Lead:** Overall responsibility for the Network Security and Monitoring sub-unit. Manages staff, develops and implements security policies, and reports to the Network Administrator.
2. **Security Engineer:** Designs, implements, and maintains network security infrastructure; develops and enforces security policies and procedures. Responds to major security incidents.
3. **Security Analyst:** Monitors network traffic and security logs; analyzes security events and alerts; investigates security incidents; creates reports.
4. **Network Monitoring Specialist:** Monitors network performance using NMS (Network Management System); sets up and configures monitoring tools; analyzes data and generates reports.

4. Line of Command and Reporting:

1. All Network Security and Monitoring staff report to the Network Security and Monitoring Lead.
2. The Network Security and Monitoring Lead reports to the Network Administrator.
3. The Network Administrator reports to the Head of the NOC.
4. The Head of the NOC reports to the Director, COMSIT.

5. Processes and Procedures:

1. **Security Policy Enforcement:** Security policies are clearly defined, communicated, and enforced. Regular training and awareness programs are conducted for all users.
2. **Threat Detection and Prevention:** Firewalls, intrusion detection/prevention systems (IDS/IPS), and other security tools are deployed and managed effectively. Regular vulnerability scans are performed.
3. **Security Monitoring:** Continuous monitoring of network traffic, security logs, and system events is conducted using SIEM (Security Information and Event Management) and other monitoring tools. Alerts are reviewed and investigated promptly.
4. **Incident Response:** A documented incident response plan is in place and followed for all security incidents. This plan includes escalation procedures, communication protocols, and post-incident analysis.
5. **Vulnerability Management:** A vulnerability management program is implemented to identify, assess, and remediate network vulnerabilities.
6. **Security Auditing:** Regular security audits are conducted to verify the effectiveness of security controls.
7. **Compliance:** The Network Security and Monitoring team ensures compliance with all relevant University policies, industry standards (e.g., NIST Cybersecurity Framework), and legal regulations.

6. Escalation Matrix:

Issue Type	Level 1 (Analyst)	Level 2 (Engineer)	Level 3 (Lead/COMSIT Security Team)
Suspicious network activity	Investigate and analyze	Escalate if malicious activity	Full incident response investigation
Security alerts	Investigate and triage	Escalate if critical	Full incident response investigation
Security incidents (minor)	Respond and remediate	Escalate if unresolved	Full incident response investigation
Security incidents (major)	Escalate immediately	Coordinate response	Full incident response investigation

Issue Type	Level 1 (Analyst)	Level 2 (Engineer)	Level 3 (Lead/COMSIT Security Team)
System compromise suspected	Escalate immediately	Coordinate response	Full incident response investigation

7. Performance Measurement: KPIs (Key Performance Indicators) are used to monitor the effectiveness of the Network Security and Monitoring sub-unit:

1. **Security Incident Response Time:** Defined targets for responding to and resolving security incidents based on severity.
2. **Mean Time To Detection (MTTD):** Track the average time it takes to detect security incidents.
3. **Mean Time To Resolution (MTTR):** Track the average time it takes to resolve security incidents.
4. **Number of Security Vulnerabilities:** Track the number of vulnerabilities identified and remediated.
5. **Network Uptime due to Security:** Track network downtime caused by security incidents.
6. **Accuracy of Security Audits:** Ensure 100% accuracy of security audit reports.
7. **False Positive Rate:** Minimize false positives from security monitoring systems.

STANDARD OPERATING PROCEDURE (SOP)

1. Purpose: This SOP defines the processes and procedures for managing and maintaining the University's servers and data, ensuring high availability, performance, security, and data integrity. It directly supports the strategic goals of the NOC and COMSIT.
2. Scope: This SOP covers all aspects of server and data management, including:

1. **Server provisioning and Management:** Managing the lifecycle of servers, including procurement, installation, configuration, maintenance, and decommissioning.
2. **Data Management:** Implementing and maintaining data management policies and procedures, including backup and recovery, data storage, and access control.
3. **Database Administration:** Managing and maintaining databases, including performance tuning, security, and backups.
4. **System Monitoring:** Continuous monitoring of server health and performance.
5. **Incident Response:** Handling server and data-related incidents according to established procedures.
6. **Capacity Planning:** Ensuring sufficient server and storage capacity to meet current and future needs.
7. **Security:** Implementing and maintaining appropriate security measures for servers and data.

3. **Roles and Responsibilities:**

8. **Server and Data Management Lead:** Overall responsibility for the Server and Data Management sub-unit. Develops and implements strategies, manages staff, and reports to the Network Administrator.
9. **System Administrators:** Manage and maintain servers, operating systems, applications, and databases. Perform regular maintenance tasks, implement security measures, and resolve server-related incidents.
10. **Database Administrators:** Manage and maintain databases, ensuring data integrity and availability. Perform regular backups and implement recovery procedures. Optimize database performance and security.
11. **Data Center Technician:** Responsible for the physical maintenance of the server room, including power, cooling, and environmental monitoring.

4. Line of Command and Reporting:

1. All Server and Data Management staff report to the Server and Data Management Lead.
2. The Server and Data Management Lead reports to the Network Administrator.
3. The Network Administrator reports to the Head of the NOC.
4. The Head of the NOC reports to the Director, COMSIT.

5. Processes and Procedures:

1. **Server Provisioning:** A standardized process for procuring, installing, configuring, and deploying servers is followed. This includes documentation of all configurations and settings.
2. **Server Maintenance:** Regular preventative maintenance tasks are scheduled and performed, including patching, software updates, and performance monitoring.
3. **Data Backup and Recovery:** A robust backup and recovery plan is implemented, including regular backups, testing of backups, and disaster recovery procedures.
4. **Data Storage:** Data storage policies and procedures are established and followed, including data retention policies and archiving strategies.
5. **Access Control:** Appropriate access control measures are implemented to protect server and data security.
6. **Database Administration:** Database performance is monitored and optimized. Regular database backups are performed. Security measures are implemented to protect database integrity and availability.
7. **System Monitoring:** Server health and performance are continuously monitored using appropriate tools. Alerts are reviewed and investigated promptly.

8. **Incident Response:** A documented incident response plan is in place for handling server and data-related incidents. This plan includes escalation procedures, communication protocols, and post-incident analysis.
9. **Capacity Planning:** Regular capacity planning is conducted to ensure sufficient server and storage capacity to meet current and future needs.
10. **Security:** Security measures are implemented to protect server and data security, including access control, encryption, and regular security audits.

6. Escalation Matrix:

Issue Type	Level 1 (System Admin)	Level 2 (DBA/Lead)	Level 3 (NOC Management/COMSIT)
Minor server issues	Troubleshoot and resolve	Escalate if unresolved	Escalate only if critical impact
Major server outages	Escalate immediately	Immediate troubleshooting	Incident Management Team
Database performance issues	Troubleshoot and optimize	Escalate if unresolved	Database Administrator Team
Data loss or corruption	Escalate immediately	Initiate data recovery	Incident Management Team
Security incidents	Escalate immediately	Coordinate response	Incident Management Team

7. Performance Measurement: KPIs (Key Performance Indicators) are used to monitor the effectiveness of the Server and Data Management sub-unit:

1. **Server Uptime:** Target should be set based on industry best practices and SLAs (e.g., 99.99%).
2. **Database Uptime:** Target for database availability (e.g., 99.9%).
3. **Backup and Recovery Success Rate:** Track the success rate of backups and recoveries.
4. **Mean Time To Repair (MTTR):** Defined targets for resolving server outages based on severity.
5. **Mean Time To Recovery (MTTR):** Defined targets for recovering from data loss or corruption incidents.
6. **Data Loss Rate:** Track instances of data loss due to server failures or other incidents. Aim for 0%.
7. **Compliance with Data Backup and Retention Policies:** Ensure 100% adherence to policies.

8. Review and Updates: This SOP will be reviewed and updated at least annually, or more frequently as needed, to reflect technological advancements, changes to the server and data

infrastructure, and evolving organizational requirements. Regular reviews with stakeholders should be incorporated.

STANDARD OPERATING PROCEDURE (SOP) FOR HELP DESK SUPPORT

1. Purpose: This SOP outlines the processes and procedures for providing efficient and effective technical support to University of Ilorin users. It aims to ensure high user satisfaction and aligns with the overall strategic goals of the NOC and COMSIT.

2. Scope: This SOP covers all aspects of Help Desk support, including:

1. **Incident Management:** Handling and resolving user-reported IT incidents.
2. **Request Fulfillment:** Processing and fulfilling user requests for IT services.
3. **Knowledge Management:** Creating and maintaining a knowledge base of solutions to common IT issues.
4. **Communication:** Communicating effectively with users regarding IT support issues.
5. **Escalation:** Escalating complex issues to higher-level support teams.
6. **Performance Monitoring:** Tracking key metrics to measure Help Desk performance.

3. Roles and Responsibilities:

1. **Help Desk Manager:** Overall responsibility for the Help Desk. Manages staff, develops and implements support procedures, and reports to the Network Administrator.
2. **Help Desk Analysts (Tier 1):** Provide first-level support to end-users, troubleshooting common issues, creating and managing tickets within the ITSM (IT Service Management) system, and escalating complex issues to Tier 2 support.
3. **Second-Level Support (Tier 2):** Provide in-depth troubleshooting and technical support for complex issues. Collaborate with other IT units as needed.

4. Line of Command and Reporting:

1. All Help Desk staff report to the Help Desk Manager.
2. The Help Desk Manager reports to the Network Administrator.
3. The Network Administrator reports to the Head of the NOC.
4. The Head of the NOC reports to the Director, COMSIT.

5. Processes and Procedures:

1. **Incident Logging and Tracking:** All incidents are logged in the ITSM system, including detailed descriptions, user information, and priority levels. Tickets are assigned and tracked throughout the resolution process.
2. **Incident Resolution:** Help Desk Analysts follow established troubleshooting procedures to resolve incidents. Documentation of the resolution process is required for all incidents.

3. **Request Fulfillment:** User requests for IT services (e.g., account creation, software installation) are processed and fulfilled according to established procedures.
4. **Knowledge Management:** A knowledge base is maintained containing solutions to frequently encountered IT issues. Help Desk Analysts are encouraged to contribute to the knowledge base.
5. **Communication:** Effective communication with users is essential. Help Desk Analysts should provide regular updates on incident status and clearly explain technical issues in non-technical terms.
6. **Escalation:** Complex or unresolved incidents are escalated to Tier 2 support or other specialized teams according to the escalation matrix.
7. **Performance Monitoring:** Key performance indicators (KPIs) are tracked and analyzed to measure Help Desk performance, such as average resolution time, customer satisfaction, and first-call resolution rate. Regular reports are generated.

6. Escalation Matrix:

Issue Type	Tier 1 (Analyst)	Tier 2 (Second-Level Support)	Level 3 (Specialized Team/NOC Management)
Simple software issues	Resolve directly	Escalate if unresolved	Not usually required
Basic hardware problems	Resolve directly or escalate	Resolve or escalate to vendor	Escalate only if critical impact
Network connectivity issues	Escalate to Network team	Further investigation	Network Infrastructure Team
Account access issues	Resolve directly	Escalate if unresolved	Identity and Access Management Team
Complex technical issues	Escalate immediately	Investigate and resolve	Relevant specialized team or NOC Management
Security incidents	Escalate immediately	Investigate and escalate	Security Team

7. Performance Measurement: KPIs (Key Performance Indicators) are used to monitor the effectiveness of the Help Desk:

1. **Average Resolution Time:** Target for resolving incidents (e.g., under 2 hours for high priority, under 4 hours for normal priority).
2. **Customer Satisfaction:** Measured through surveys or feedback mechanisms. Target should be 90% or higher.
3. **First Call Resolution Rate:** Percentage of incidents resolved on the first contact. Target should be 70% or higher.
4. **Ticket Resolution Accuracy:** Percentage of tickets resolved correctly on the first attempt. Target should be above 95%.

5. **Number of Escalated Tickets:** Track percentage of tickets escalated to higher levels. Aim for a low percentage.

8. Review and Updates: This SOP will be reviewed and updated at least annually, or more frequently as needed, to reflect changes in technology, user needs, and organizational requirements. Regular reviews with stakeholders should be incorporated.

STANDARD OPERATING PROCEDURE (SOP) FOR POWER AND COOLING ADMINISTRATION SUB UNIT

1. Purpose: This SOP defines the processes and procedures for managing and maintaining the power and cooling infrastructure of the University of Ilorin NOC, ensuring reliable and stable operation of IT equipment. This directly supports the overall strategic goals of the NOC and COMSIT.

2. Scope: This SOP covers all aspects of power and cooling administration, including:

1. **Power Infrastructure Management:** Maintaining the primary and backup power systems, including generators, UPS (Uninterruptible Power Supply) systems, and power distribution.
2. **Cooling Infrastructure Management:** Maintaining the HVAC (Heating, Ventilation, and Air Conditioning) systems and other cooling equipment to regulate temperature and humidity within the NOC.
3. **Environmental Monitoring:** Continuous monitoring of environmental conditions (temperature, humidity, airflow) within the NOC.
4. **Preventive Maintenance:** Implementing and adhering to a preventative maintenance schedule for all power and cooling equipment.
5. **Incident Response:** Handling power and cooling-related incidents according to established procedures.

3. Roles and Responsibilities:

1. **Power and Cooling Administration Lead:** Overall responsibility for the Power and Cooling Administration sub-unit. Develops and implements strategies, manages staff, and reports to the Network Administrator.
2. **Power and Cooling Engineer:** Designs, implements, and maintains the NOC's power and cooling systems; develops and implements preventative maintenance plans; responds to power and cooling system alerts; performs troubleshooting; monitors environmental conditions.
3. **Power and Cooling Technician:** Performs routine maintenance on power and cooling equipment; assists the engineer with more complex tasks.

4. Line of Command and Reporting:

1. All Power and Cooling Administration staff report to the Power and Cooling Administration Lead.
2. The Power and Cooling Administration Lead reports to the Network Administrator.
3. The Network Administrator reports to the Head of the NOC.
4. The Head of the NOC reports to the Director, COMSIT.

5. Processes and Procedures:

1. **Power System Maintenance:** Regular preventative maintenance is performed on all power equipment, including generators, UPS systems, and power distribution. This includes regular testing, inspections, and necessary repairs.
2. **Cooling System Maintenance:** Regular preventative maintenance is performed on all cooling equipment, including HVAC systems and other cooling devices. This includes regular testing, inspections, and necessary repairs.
3. **Environmental Monitoring:** Environmental conditions (temperature, humidity, airflow) within the NOC are continuously monitored using sensors and monitoring systems. Alerts are triggered if conditions exceed predefined thresholds.
4. **Preventative Maintenance Schedule:** A detailed preventative maintenance schedule is developed and implemented for all power and cooling equipment. This schedule includes specific tasks, frequencies, and responsible personnel.
5. **Incident Response:** A documented incident response plan is in place for handling power and cooling related incidents. This plan includes escalation procedures, communication protocols, and post-incident analysis.
6. **Emergency Procedures:** Procedures are in place for handling power outages and other emergencies. This includes backup power procedures and emergency contact information.
7. **Documentation:** Comprehensive documentation is maintained for all power and cooling equipment, including specifications, maintenance records, and diagrams.

6. Escalation Matrix:

Issue Type	Level 1 (Technician)	Level 2 (Engineer)	Level 3 (NOC Management/Facilities)
Minor power/cooling issues	Troubleshoot and resolve	Escalate if unresolved	Escalate only if critical impact
Major power outages	Escalate immediately	Immediate troubleshooting	Facilities Management/Emergency Services
HVAC system	Escalate	Immediate	Facilities Management

Issue Type	Level 1 (Technician)	Level 2 (Engineer)	Level 3 (NOC Management/Facilities)
malfunctions	immediately	troubleshooting	
Environmental condition alerts	Investigate and address	Escalate if unresolved	Facilities Management
Generator failure	Escalate immediately	Immediate troubleshooting	Facilities Management/Emergency Services

7. Performance Measurement: KPIs (Key Performance Indicators) are used to monitor the effectiveness of the Power and Cooling Administration sub-unit:

1. **NOC Uptime due to Reliable Power:** Track the percentage of NOC downtime caused by power outages. Aim for 0%.
2. **UPS System Availability:** Track the percentage of time the UPS system provides uninterrupted power. Aim for 100%.
3. **HVAC System Uptime:** Track the percentage of time the HVAC system maintains optimal environmental conditions. Aim for 99% or higher.
4. **Mean Time To Repair (MTTR) for Power/Cooling Outages:** Track the average time taken to resolve power or cooling system outages. Define targets based on severity.
5. **Adherence to Preventive Maintenance Schedule:** Track the percentage of preventative maintenance tasks completed according to schedule. Aim for 100%.

I. LINE OF COMMAND

I. Director, COMSIT: Overall responsibility for the Computer Services and Information Technology Directorate (COMSIT). Provides strategic direction and resource allocation to all units, including the NOC.

II. Head of NOC Unit: Reports directly to the Director, COMSIT. Provides strategic direction and oversees all operations of the NOC. Responsible for overall performance and staff management within the NOC.

III. Core Mandate Leads (Reporting to Head of NOC Unit): Each lead manages a specific core mandate, ensuring efficient workflows and adherence to SOPs. These leads are responsible for the performance of their teams and report directly to the Head of the NOC Unit.

1. **Network Infrastructure Management Lead:** Oversees all aspects of network infrastructure management, including fiber optics, LAN, and wireless. Ensures network availability, performance, and security.
2. **Network Security and Monitoring Lead:** Oversees the implementation and maintenance of network security infrastructure and monitoring systems. Develops and implements security policies and procedures.

3. **Server and Data Management Lead:** Responsible for all server-related operations, including maintenance, security, access control, and data management. Ensures high server availability and data integrity.
4. **Help Desk and Support Lead:** Oversees all Help Desk operations, ensuring timely and efficient issue resolution. Manages staff, develops training programs, and monitors customer satisfaction.
5. **Power and Cooling Administration Lead:** Oversees the management and maintenance of the NOC's power and cooling systems, ensuring optimal environmental conditions and preventing outages.
6. **Technical Staff (Reporting to Core Mandate Leads):** These are the individuals performing the day-to-day tasks within each core mandate. Their roles and responsibilities are defined within the individual SOPs for each sub-unit.
7. **Network Infrastructure Management:** Network Architect, Senior Network Engineers, Network Engineers, Network Technicians.
8. **Network Security and Monitoring:** Security Engineer, Security Analyst, Network Monitoring Specialist.
9. **Server and Data Management:** System Administrators, Database Administrators, Data Center Technician.
10. **Help Desk and Support:** Help Desk Manager, Help Desk Analysts (Tier 1), Second-Level Support (Tier 2).
11. **Power and Cooling Administration:** Power and Cooling Engineer, Power and Cooling Technician.
12. **Operations Manager (Optional):** Depending on the size and structure of the NOC, an Operations Manager could be included to provide additional oversight and coordination between the Core Mandate Leads, reporting to the Head of the NOC Unit.
13. **Key Considerations:**
14. **Span of Control:** The number of individuals reporting to each manager should be carefully considered to ensure effective management and avoid overburdening any single individual.
15. **Communication:** Clear communication channels should be established between all levels of the organization.
16. **Accountability:** Clear lines of responsibility should be defined for all tasks and decisions.
17. **Flexibility:** The structure should be flexible enough to adapt to changing needs and priorities.

This Line of Command provides a clear hierarchical structure for the NOC. Regular reviews and adjustments may be necessary as the NOC evolves and its operational needs change. Remember that this is a recommendation; the specific structure should be tailored to the University of Ilorin's needs and resources after careful consideration by relevant stakeholders.

I. DOCUMENT CONTROL

1. **Version:**
2. **Effective Date:**
3. **Review Due Date:**
4. **Prepared by:**
5. **Approved by:**
6. **Distribution:**

    1. Head of NOC Unit
    2. Core Mandate Leads (Network Infrastructure Management, Network Security & Monitoring, Server & Data Management, Help Desk & Support, Power & Cooling Administration)
    3. Relevant Technical Staff within each Sub-unit
    4. Network Administrator
    5. Deputy Directors, COMSIT
    6. Director, COMSIT
    7. [Add any other relevant stakeholders as needed)

7. Revision History:

K. FUTURE EXPANSION PLAN

A future expansion plan for the University of Ilorin's Network Operations Center (NOC) should be a dynamic, evolving document, regularly reviewed and updated. It should align with the University's overall IT strategic plan and consider factors such as technological advancements, budgetary constraints, and evolving user needs.

Here's a framework for a future expansion plan for the NOC, incorporating best practices to address potential challenges identified in the provided documents:

I. Expansion Strategies:

1. **Fiber-Optic Network Expansion:** Complete the transition to a full fiber-optic network infrastructure to improve reliability, scalability, and bandwidth. Prioritize areas with limited or no fiber connectivity.
2. **Wireless Network Enhancement:** Expand and upgrade the wireless network infrastructure to address coverage gaps and improve performance, especially in high-density areas. Consider deploying additional enterprise-grade wireless radios and implementing technologies like Wi-Fi 6E.
3. **Data Center Modernization:** Upgrade the data center infrastructure to support future growth and technological advancements. This may include transitioning to licensed virtualization, implementing high-level firewalls, and adopting cloud-based solutions.

4. **Network Management System (NMS) Upgrade:** Implement or upgrade the NMS to enhance monitoring capabilities, provide more detailed performance metrics, and improve proactive identification and resolution of issues.
5. **Security Enhancements:** Invest in advanced security tools and technologies, such as next-generation firewalls, intrusion detection/prevention systems, and security information and event management (SIEM) systems. Implement robust security policies and procedures.
6. **Staff Development:** Invest in training and certification programs for NOC staff to enhance their skills and expertise in areas such as network engineering, security, and data management.

II. Resource Allocation:

1. **Budgetary Requirements:** Develop a detailed budget outlining the costs associated with each expansion project. Explore funding opportunities from government grants, private donations, or internal reallocation of funds.
2. **Personnel Requirements:** Determine the staffing needs for each expansion project. Consider hiring additional personnel with specialized skills in areas such as network engineering, security, and data management.
3. **Technology Procurement:** Develop a plan for procuring and implementing new technologies and equipment. Consider factors such as compatibility, scalability, and vendor support.

III. Implementation Timeline:

1. **Phased Approach:** Implement the expansion plan in phases, prioritizing projects based on their impact and feasibility. This allows for iterative development and adaptation based on feedback and results.
2. **Project Management:** Use project management methodologies to ensure that projects are completed on time and within budget. Establish clear timelines, milestones, and responsibilities.

I. Internal Communication Plan:

. **Purpose:** To facilitate efficient information sharing and collaboration within the NOC and COMSIT.

a. **Methods:**

    1. Regular meetings: Team meetings, operational reviews, and project status updates. Use agendas and minutes to ensure clarity and accountability.

2. Instant messaging/collaboration tools: Utilize platforms like Slack, Microsoft Teams, or similar for quick communication and information sharing among team members.
3. Email: For formal communications, announcements, and distributing reports.
4. Intranet/Knowledge base: Maintain an internal knowledge base to store and share information about processes, procedures, and troubleshooting tips.
5. Internal communication platform: Consider a dedicated platform for announcements, updates, and news related to the NOC.

II. COMMUNICATION PLAN:

. **Purpose:** To keep university users, vendors, and other external stakeholders informed about NOC services, incidents, and planned maintenance.

a. **Methods:**

1. University Website: Provide information on NOC services, contact information, and service status updates on the University website.
2. Email: Used to communicate planned maintenance, service disruptions, and other important information to university users. Segmentation of the mailing list is important to ensure efficient distribution and prevent information overload.
3. IT Service Management (ITSM) System: Utilize a centralized ITSM system (like ServiceNow) for tracking, managing, and resolving user-reported incidents. This provides a central repository for all IT-related issues and provides updates to users.
4. Social Media (if appropriate): Use social media channels (e.g., Twitter, Facebook) to disseminate information to a wider audience.
5. Newsletters/Announcements: Periodic newsletters or announcements can keep users informed of significant changes or upgrades to NOC services.
6. Vendor Communication Channels: Establish clear communication channels with vendors for reporting issues, requesting support, and managing contracts. Use SLAs (Service Level Agreements) to clearly define response times and expectations.

III. Communication Protocols:

1. **Incident Management:** A clear escalation path and communication protocol should be established for handling incidents. This should include defined roles and responsibilities, escalation procedures, and communication methods (e.g., phone, email, instant messaging).

2. **Change Management:** A similar protocol should be in place for communicating planned changes to the network infrastructure. This should include notification to users about potential service disruptions and mitigation strategies.

0. **Scheduled Maintenance:** Users should be notified in advance about scheduled maintenance activities, including the expected duration and potential impacts.

0. **Emergency Response:** Define clear communication protocols for emergency situations such as major outages.

1. **Formal Communication:** For official communication regarding security breaches or critical incidents, establish formal channels involving appropriate stakeholders (e.g., university administration, legal counsel, law enforcement).

INTERFACING WITH OTHER COMSIT UNITS

I. Incident Management Process:

1. **User Reports Incident:** (User) → Reports incident via phone, email, or ITSM system.
2. **Help Desk (NOC) Receives Incident:** (Help Desk) → Logs incident in ITSM, determines priority.
3. **Incident Classification:** (Help Desk) → Is the incident network-related?

- **Yes:** Proceed to step 4.
- **No:** Escalate to appropriate COMSIT unit (Software Development, Software & Hardware Inst., etc.).

Network Issue Identification: (NOC - Network Infrastructure Management) → Identifies root cause of network-related incident.
Incident Resolution: (Relevant NOC Sub-unit) → Resolves incident (Network Infrastructure, Security, etc.).
Incident Closure: (Help Desk) → Closes incident in ITSM; updates user.
Post-Incident Review: (NOC Management & relevant COMSIT units) → Reviews incident, identifies improvements needed.

II. Change Management Process:

1. **Change Request:** (Any COMSIT unit or user) → Submits change request via established process.
2. **Change Request Review:** (NOC Management) → Reviews change request, assesses impact on network.

3. **Impact Assessment:** (NOC Management, relevant COMSIT units) → Determines potential impact on other COMSIT units; collaborates as needed (e.g., Web Services for website changes).
4. **Change Approval:** (Head of NOC, relevant COMSIT managers) → Approves or rejects change request based on impact assessment.
5. **Change Implementation:** (Relevant NOC sub-unit) → Implements change.
6. **Testing and Verification:** (Relevant NOC sub-unit, other COMSIT units as needed) → Tests the implemented change.
7. **Change Closure:** (NOC Management) → Closes change request; updates stakeholders.
8. **Post-Implementation Review:** (NOC Management & relevant COMSIT units) → Reviews change implementation, identifies improvements.

III. Preventive Maintenance Process:

1. **Maintenance Schedule Development:** (NOC Management, Power & Cooling Admin) → Creates a preventative maintenance schedule for network devices and infrastructure, including power and cooling systems.
2. **Schedule Approval:** (Head of NOC) → Approves maintenance schedule.
3. **Maintenance Execution:** (Relevant NOC sub-units, Software & Hardware Inst. & Repair) → Performs scheduled maintenance.
4. **Documentation:** (Relevant NOC sub-units) → Records all maintenance activities.

IV. Capacity Planning Process:

1. **Capacity Needs Assessment:** (NOC Management, Software Development, other COMSIT units) → Assesses future capacity needs for network, servers, and storage.
2. **Capacity Planning:** (NOC Management) → Develops a capacity plan.
3. **Resource Allocation:** (COMSIT Administration & Operations) → Allocates resources based on the capacity plan.
4. **Implementation:** (Relevant NOC sub-units) → Implements capacity expansion.

V. Security Management Process:

1. **Security Policy Development:** (NOC Security & Monitoring, Cybersecurity) → Develops and maintains network security policies and procedures.
2. **Policy Implementation:** (NOC Security & Monitoring, other COMSIT units) → Implements security policies and procedures across all COMSIT units.
3. **Security Audits:** (NOC Security & Monitoring, Cybersecurity) → Conducts regular security audits.
4. **Vulnerability Management:** (NOC Security & Monitoring, Cybersecurity) → Identifies and remediates network vulnerabilities.

5. **Security Awareness Training:** (Cybersecurity, NOC, Help Desk) → Provides security awareness training to all COMSIT staff and users.

O. CONCLUSION

The blueprint for the NOC at the University of Ilorin not only outlines a clear operational framework but also sets ambitious goals for achieving technological excellence. By leveraging its strengths, addressing weaknesses, seizing opportunities, and mitigating threats, the NOC is well-positioned to enhance the university's digital infrastructure. This strategic initiative will ultimately contribute to a more connected, secure, and efficient campus environment that supports academic success and innovation. The commitment to aligning with global best practices ensures that the University of Ilorin remains competitive in an increasingly digital world.

Portal Unit

A. OPERATIONAL BRIEF

The Portal unit shall be responsible for day-to-day operations of all portals of the University with an appointed Desk-Officer for each portal by the Head of portal team who must not be below the rank of Deputy Director. This unit shall interact with Software and Applications Development, Web, Mail Services and Help-desk units from time to time in ensuring quality of service

B. INTRODUCTION:

The Portal Unit in a university system (University of Ilorin) is dedicated to managing and maintaining the university's online portals, which serve as central hubs for accessing a variety of academic, administrative, and support services. These portals provide students, faculty, and staff with a unified, secure interface to access essential information, including course materials, grades, schedules, and university announcements.

Key responsibilities of the Portal Unit include the design and development of user-friendly interfaces, integration with other university systems (such as learning management systems and administrative databases), and ensuring the availability and reliability of portal services. The unit also plays a crucial role in implementing security measures to protect sensitive information and providing technical support to users.

The Portal Unit aims to enhance the digital experience of members of the university community by streamlining access to resources and services, promoting efficient communication, and supporting the university's overall mission of teaching, research and community services.This unit is essential in facilitating the day-to-day operations of the university, fostering engagement, and improving the accessibility of information and services for all users.

C. MISSION STATEMENT

The Portal Unit is expected to streamline access to academic, administrative, and support services, enhancing the digital experience and promoting efficient communication within the university ICT ecosystem.

D. STAFFING :

1. Head of Unit (1):

   i. Oversees the overall operations of the unit;
   ii.Sets strategic goals inline with university strategic plan:
   iii. Responsible for project management, team leadership, and stakeholder communication.

0. Web Developer(4):

    i. Develops, maintains, and updates the portal' front-end and back-end components.

    ii. Ensures compatibility with various devices and browsers and works on user interface (UI) and user experience (UX) improvements.

0. Systems Administrator(1):
    i. Manages server infrastructure, including hosting environments, database management, and security.
    ii. Ensures the reliability, performance, and security of portal systems.

0. IT Support Specialist(8):

    i. Provides technical support to users of the portal, resolving issues related to access, navigation, and functionality.

    ii. Conducts user training and documentation.

    0. Content Manager(1):
    i. Responsible for the organization, quality, and accuracy of content on the portal.
    ii.Works with various departments to ensure content is up-to-date and relevant.

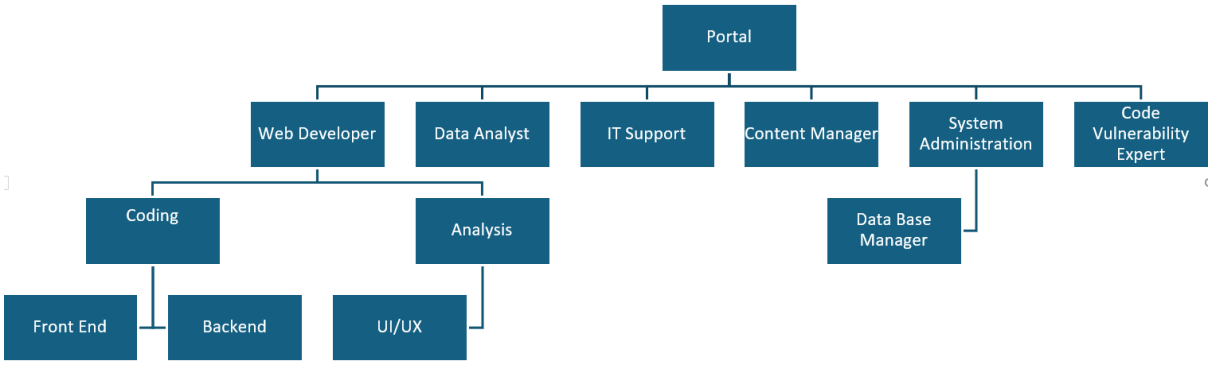
    0. Data Analyst(3):

    i.Analyzes user data and system metrics to inform decisions on improvements and new features.

    ii. Monitors portal usage trends and provides insights for optimization.

0. Code Vulnerability Expert(1):
    i. Focuses on protecting the portal from cybersecurity threats.
    ii. Conducts regular security assessments, manages access controls, and ensures compliance with data protection regulations.

E. Unit Organogram



F. SWOT ANALYSIS

A SWOT analysis helps identify internal strengths and weaknesses, as well as external opportunities and threats, for a University Portal Unit. This information can be used to inform strategic planning and decision-making.

i. Strengths

1. **Centralized Enterprise Platform:** The portal serves as a centralized enterprise platform for accessing a wide range of academic resources, administrative services, and communication tools, by providing convenience and efficiency for users. It provides opportunity for mapping the entire university thereby creating expected synergies among inter-related units of the university.
2. **User-Friendly Interface:** The unit offers a user-friendly interface through an enterprise portal that is easy to navigate, ensuring effortless users experience with increased perceived ease of use.
3. **Integrated Platform:** It affords the opportunity of integrating all the university portal system with a single user sign-on. This provides a more synergise and cost-effective operations within the university ICT ecosystem.

4. **Secured Platform:** The unit implements robust security measures to protect sensitive data and prevent unauthorized access, ensuring compliance with privacy regulations and maintaining trust in the system.
5. **Responsive Support:** The unit provides responsive technical support to address user inquiries, troubleshoot issues, and provide guidance on utilizing portal features effectively, enhancing user experience and satisfaction.
6. **Continuous Improvement:** There is a culture of continuous improvement within the unit, with regular updates and enhancements based on user feedback, technological advancements, and best practices in digital platforms.
7. **Training and Documentation:** The unit offers comprehensive training resources and documentation to educate users on portal functionalities, increasing adoption rates and minimizing user frustrations.

ii. **Weaknesses**

1. **Technical Issues:** The portal unit may experience technical glitches, downtime, or performance issues, leading to frustration and disruption for users trying to access essential resources or complete administrative tasks.
2. **Limited Integration:** While the portal integrates with various university systems, there may be limitations in the extent of integration or interoperability with external platforms or third-party applications, hindering seamless data exchange and functionality.
3. **Complexity of Features:** The abundance of features and functionalities within the portal may lead to complexity for some users, especially those who are less tech-savvy or unfamiliar with navigating digital platforms.
4. **Accessibility Challenges for Users with Special Needs:** The portal's interface and content may not fully adhere to accessibility standards, posing challenges for users with disabilities in accessing and utilizing the platform effectively.
5. **Training Gaps:** Despite offering training resources, there may be gaps in the provision of comprehensive and accessible training for users, leading to underutilization of portal features and suboptimal user experiences.
6. **Security Vulnerabilities:** Despite implementing security measures, the portal unit may still be vulnerable to cybersecurity threats such as data breaches, phishing attacks, or malware infections, posing risks to the confidentiality and integrity of sensitive information. Thus, continuous investment on security is necessary.
7. **Resistance to Change:** Some users, particularly long-time staff or faculty, may resist adopting new features or workflows within the portal, preferring traditional methods or being resistant to embrace technological advancements.

8. **Scalability Challenges:** As the university grows or experiences fluctuations in user demand, the portal unit may face challenges in scaling its infrastructure and resources to accommodate increasing traffic and usage patterns effectively.

iii. **Opportunities:**

1. **Enhanced Mobile Experience:** With the increasing use of mobile devices for accessing information and conducting tasks, there's an opportunity to optimize the portal for mobile responsiveness and develop dedicated mobile apps to improve accessibility and convenience for users on the go.
2. **Integration with Emerging Technologies:** Exploring integration with emerging technologies such as artificial intelligence, machine learning, and chatbots can enhance the functionality and intelligence of the portal, providing personalized recommendations, automated support, and predictive analytics to users.
3. **Expanded Collaboration Features:** Introducing advanced collaboration features such as real-time document editing, video conferencing, and project management tools within the portal can facilitate seamless teamwork and communication among students, faculty, and staff, fostering a culture of collaboration and innovation.
4. **Data Analytics and Insights:** Leveraging data analytics capabilities within the portal can provide valuable insights into user behaviour, preferences, and trends, enabling informed decision-making, targeted interventions, and personalized experiences for users.
5. **Integration with External Platforms:** Strengthening integration with external platforms such as job portals, research databases, and industry-specific tools can enrich the portal's offerings and provide added value to users by expanding access to relevant resources and opportunities.
6. **Community Engagement Initiatives**: Implementing community engagement initiatives within the portal, such as online forums, virtual events, and peer-to-peer support networks, can foster a sense of belonging and connectedness among members of the university community, enhancing overall engagement and satisfaction.
7. **Accessibility Improvements:** Investing in accessibility enhancements such as screen reader compatibility, alternative text descriptions, and keyboard navigation options can ensure inclusivity and accessibility for users with disabilities, aligning with regulatory requirements and promoting diversity and equity within the university.
8. **Partnerships and Collaborations:** Forming partnerships and collaborations with other institutions, organizations, and technology vendors can expand the capabilities and resources of the portal unit, enabling access to cutting-edge

technologies, expertise, and funding opportunities to support innovation and growth.

iv. **Threats**

1) Cybersecurity Risks: The increasing risk of cyberattacks and data breaches, requiring robust security measures.
2) Technological Obsolescence: The need to constantly adapt to new technologies and trends, requiring ongoing investment and training.
3) Budget Constraints: Inadequate funding that could limit the unit's ability to maintain and improve the portal.
4) Regulatory Compliance: Non-compliance to various educational and governmental regulatory framework can lead to legal challenges, penalties, and loss of trust among users.
5) User Resistance and Adoption Challenges: Users may resist adopting a new portal, especially if it requires a steep learning curve.
6) Data Security and Privacy Concerns: If the portal is not securely designed, it becomes a target for cyberattacks, such as data breaches, hacking, and unauthorized access.

G. KEY PERFORMANCE INDICATORS (KPIS) FOR PORTAL UNIT ROLES

1) Portal Unit Head

Project Delivery Timeliness: Percentage of projects completed over a period of time.

Stakeholder Satisfaction: Survey-based usability evaluation on perceived usefulness and perceived ease of use.

Team Productivity: Overall output and efficiency of the team over a period of time.

2) System Developer

System Uptime: Percentage of time the portal is fully operational and accessible over a period of time.

Bug Resolution Time: Average time taken to fix reported issues or bugs.

Feature Deployment Frequency: Number of new features or updates released within a specified period of time.

3) Systems Administrator

Server Uptime: Percentage of time servers are fully operational and stable over a period of time.

Incident Response Time: Average time it takes to respond to and resolve server-related issues(between when the issue is escalated and resolved).

Backup and Recovery Success Rate: Percentage of successful backups and recovery tests over a period of time.

4) **IT Support Specialist**

First Call Resolution Rate: Percentage of support issues resolved on the first level of escalation.

Average Resolution Time: Average time taken to resolve an issue (in a raised ticket)over a period of time(between when issue is escalated and resolved.

User Satisfaction: User feedback ratings on support services provided over a period of time.

5) **Content Manager**

Content Accuracy Rate: Percentage of content free of errors or outdated information.

Update Frequency: Number of content updates made over a period of time.

Content Engagement Metrics: Metrics such as page views, time spent on page, and user feedback.

6) **Data Analyst**

Data Accuracy and Integrity: Percentage of data in-accuracy and security over a period of time.

Insight Delivery Timeliness: Time taken to deliver actionable insights or reports over a period of time.

Usage Analysis Reports: Frequency and quality of reports on portal usage patterns and trends over a period of time.

7) Code Vulnerability Expert

Incident Response Time: measurement of the time between when vulnerability is escalated, and resolved.

Security Breach Rate: Number of security breaches or vulnerabilities detected and resolved over a pre-defined period of time.

Compliance Audit Success Rate: Rate of compliance with data protection and cybersecurity standards.

H. STANDARD OPERATING PROCEDURE (SOP).

1. Introduction

The Portal Unit is responsible for managing the university's online portals, ensuring they are reliable, secure, and user-friendly. This SOP outlines the procedures for operations, reporting, escalation, job descriptions, line of command, and responsibilities within the unit.

2. Organizational Structure

1. **Head, Portal Unit:** Overall head, responsible for strategic direction and operations.
2. **Web Developers:** Responsible for the development and maintenance of portal systems.
3. **Systems Administrator:** Manages server infrastructure and ensures system stability.
4. **IT Support Specialists:** Provide technical support and user assistance.
5. **Content Manager:** Oversees portal content management.
6. **Data Analyst:** Analyzes usage data and provides insights.
7. **Security Analyst:** Ensures the security and compliance of portal systems.

3. Reporting Structure

Daily Reports: Team members report daily progress and issues to the Portal Unit Head.

Weekly Reports: The Portal Unit Head prepares a summary of activities and issues for the Director of COMSIT.

Monthly Reports: A comprehensive report including KPIs, major projects, incidents, and resolutions, is submitted to COMSIT.

4. Escalation Procedure

Level 1: Issues are initially handled by IT Support Specialists. If unresolved within 4 hours, they escalate to the relevant specialist (Web Developer, Systems Administrator, etc.).

Level 2: If an issue persists for more than 24 hours or involves significant disruption, it is escalated to the Head of Portal Unit.

Level 3: For critical incidents that impact university-wide operations or data security, the Portal Unit Head escalates the issue to the Director of COMSIT.

I. LINE OF COMMAND

Primary Line: IT Support Specialists → Web Developers/Systems Administrator/Content Manager → Portal Unit Head → Director of COMSIT

Emergency Line: For critical incidents, direct reporting from any team member to the Portal Unit Head.

J. DOCUMENT CONTROL

1. Version:
2. Effective Date:
3. Review Due Date:
4. Prepared by:
5. Approved by:
6. Distribution:

Version Control: This SOP document is maintained by the Portal Unit Head. Any changes must be documented with a new version number and date.

7. Revision history

K. FUTURE EXPANSION PLANS

The University Portal Unit should have a dynamic road map for future expansion to ensure the portal remains a valuable and relevant resource for the university community. The framework will outline those plans:

User-Centricity: Prioritize user needs and feedback in all expansion plans.

Innovation: Embrace new technologies and approaches to enhance the portal experience.

Scalability: Ensure the portal can handle increasing traffic and data volume as the university grows.

Integration: Seek opportunities to integrate with other university systems and services.

Accessibility: Maintain and improve accessibility for all users, including those with disabilities.

Security: Continuously enhance security measures to protect user data and the portal itself.

L. COMMUNICATION PLAN

This plan outlines how the Portal unit will communicate with its various stakeholders, ensuring transparency, fostering collaboration, and promoting the portal's value and usage.

Keep stakeholders informed: Provide regular updates on portal development, maintenance, new features, and important announcements.

Promote portal usage: Encourage students, faculty, staff, and alumni to utilize the portal's resources and services.

Gather feedback: Establish channels for collecting user feedback and incorporating it into portal improvements.

Build relationships: Foster strong relationships with key stakeholders across the university.

Manage expectations: Communicate clearly about the portal's capabilities, limitations, and future plans.

Enhance transparency: Ensure open and accessible communication about the unit's activities and decision-making processes.

M. COMMUNICATION PROTOCOL

Internal Communication: Use of designated communication channels (email, instant messaging platforms) for daily operations and updates.

External Communication: All external communications (e.g., to other departments, stakeholders) must be approved by the Portal Unit Head.

N. PORTAL UNIT INTERFACING WITH OTHER COMSIT UNITS

Software and Applications Development Unit: The Portal Unit collaborates closely with the Software and Applications Development Unit to integrate new features and systems into the university portal. This partnership ensures that software applications developed by the university are seamlessly accessible through the portal, enhancing functionality and user experience. Regular coordination meetings help align development priorities and timelines.

Cybersecurity Unit: In collaboration with the Cybersecurity and Multimedia Unit, the Portal Unit ensures that the portal systems are secure and compliant with cybersecurity standards. This includes implementing security protocols, conducting regular security audits, penetration test and responding to potential threats. The Cybersecurity and Multimedia Unit provides the expertise needed to protect sensitive data and maintain user trust.

Training Unit: The Training Unit supports the Portal Unit by providing training sessions and resources for users. These sessions cover portal navigation, feature utilization, and best practices for data security. By educating faculty, staff, and students, the Training Unit helps maximize the portal's effectiveness and user satisfaction.

Email and Help Desk Services Unit: The Email and Help Desk Services Unit offers frontline support to users encountering issues with the portal. This unit handles user queries, troubleshooting, and ticketing, providing a direct link between the Portal Unit and end-users. They escalate unresolved issues to the Portal Unit, ensuring timely resolution.

Web Service Unit: The Portal Unit works with the Web Service Unit to manage and maintain the university’s online presence. This includes aligning the portal’s design and functionality with the broader web strategy, ensuring consistent branding, and optimizing web performance. The Web Service Unit's expertise in web standards and SEO enhances the portal's accessibility and visibility.

Faculty IT Officials: Faculty IT Officials act as liaisons between the Portal Unit and academic departments. They provide feedback on portal functionality, report specific departmental needs, and assist in the implementation of academic resources on the portal. This collaboration ensures that the portal meets the diverse requirements of various academic disciplines and enhances the faculty's ability to deliver educational content.

O. CONCLUSION:

In conclusion, the Portal Unit plays a pivotal role in the university's digital ecosystem, serving as the central hub for accessing a wide range of services and information. Through close collaboration with other COMSIT unit. The unit ensures the portal remains secured, user-friendly, and aligned with the university's goals.

Software and Applications Development Unit

A. OPERATIONAL BRIEF

The unit shall be responsible for gathering and validating of requirements of any proposed solution/automation towards seamless deployment of such solutions particularly when a new process is to be automated to achieve seamless implementation without disruption to already established university procedures. This is in line with global best practices for sustainable digital transformation. The unit will equally coordinate the process mapping project of the current Administration for proper synergies among interrelated processes. The Unit must interact with various units and organs of the university from time to time for seamless recognition of needs in terms of additional features expected to enhance our processes:

B. INTRODUCTION

The Software and Applications Development Unit (SADU) is established within the COMSIT Directorate to spearhead the automation and digital transformation efforts of the university. The primary goal of this unit is to ensure the seamless deployment of software solutions, thereby enhancing the efficiency of the University's processes without disrupting established procedures. As part of our commitment to global best practices, the SADU is instrumental in achieving sustainable digital transformation through meticulous requirement gathering, validation, and process mapping.

C: MISSION STATEMENT:

To facilitate seamless digital transformation by gathering and validating requirements for proposed solutions and automation.

D: STAFFING:

1. **Leadership and Coordination:**
   Unit Head (1 staff): Provides strategic direction and oversees all operations within the SADU.

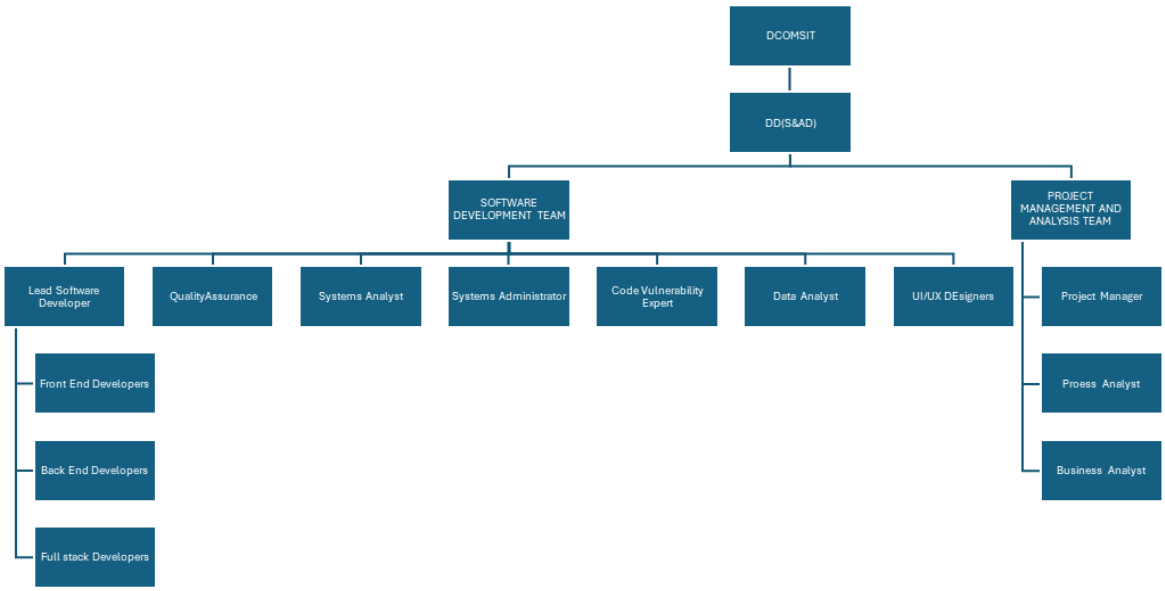
0. **Software Development Team:**
   . **Lead Software Developer**: Oversees development projects and ensures alignment with the unit's objectives.
   a. **Backend Developers**: Focus on server-side logic and integration.
   b. **Frontend Developers**: Handle the user interface and user experience design.
   c. **Full-Stack Developers**: Capable of working across both frontend and backend tasks.
   d. **Quality Assurance:** Project Validation
   e. **Systems Analysts**: Responsible for testing software to ensure quality and functionality
   f. **System Administrator:** Manages IT infrastructure and ensures system uptime.

g. **UX/UI Designers (3 staff)**: Ensure user-centric design and usability.
h. **Data Analysts (3 staff)**: Analyze data to support decision-making and optimize digital transformation efforts.
i. **Code Vulnerability Expert (1 staff)**: Ensure that software solutions adhere to security best practices and protect university data.

3. Project Management and Analysis team:

. **Project Manager (1 staff)**: Manages timelines, resources, and coordinates between teams.
a. **Business Analyst (1 Staff)**: Gather and validate requirements, and translate them into technical specifications.
b. **Process Analyst (1 staff)**: Focus on process mapping and optimization to enhance workflow efficiency.

E. Unit Organogram



F. SWOT Analysis

Strengths:

- Adequate knowledge of process automation.
- Strong understanding of the university's procedures and needs.
- Expertise in process mapping.

Weaknesses:

- Limited resources: (human, licensed software, hardware).
- Resistance to change from stakeholders accustomed to established processes.

Opportunities:

- Potential to streamline university operations and improve productivity.
- Opportunity to leverage emerging technologies for educational innovation.

Threats:
- Dynamism of digital innovations.
- Data security and privacy concerns.

G. KEY PERFORMANCE INDICATORS (KPIS)
Each role has specific job descriptions and KPIs outlined based on briefings. Performance is reviewed based on these KPIs to ensure alignment with unit goals.

1. **Project Manager:**
   KPI: Project Completion Rate: Percentage of projects delivered on time and within budget.

   KPI: Client Satisfaction: Measure of client feedback scores post-deployment.

0. **Business Analyst:**
   KPI: Requirement Accuracy: Percentage of projects where initial requirements match final delivery without significant changes.

   KPI: Stakeholder Engagement: Number of stakeholder meetings conducted and feedback incorporated.

0. **Software Developer:**
   KPI: Code Quality: Number of defects per 1000 lines of code, using code benchmarking procedures to evaluate code efficiency

   KPI: Feature Delivery: Percentage of features delivered on schedule.

Quality Assurance/ Systems Analyst:
KPI: Bug Detection Rate: Number of bugs identified and fixed before deployment.

KPI: Test Coverage: Percentage of code or features covered by tests.

System Administrator:
KPI: System Uptime: Percentage of time the systems are operational and available.

KPI: Incident Response Time: Average time taken to resolve system incidents.

Code Vulnerability Expert:
KPI: Security Incident Rate: Number of security incidents per month.

KPI: Compliance Rate: Percentage of systems and processes compliant with security standards.

Process Analyst:

KPI: Process Improvement Implementation: Number of process improvements implemented.

KPI: Efficiency Gain: Measure of time or cost savings achieved through process improvements.

UI/UX Designer:

1. User Satisfaction and Usability:
    . Measure user satisfaction through surveys or feedback forms.
    a. Assess the likelihood of users recommending the product.
    b. Use standardized questionnaires to evaluate usability.

2. Design and Development Process Efficiency:

. Measure the time taken to complete each design phase.
a. Track the time from design submission to final approval.
b. Monitor the number of revisions before approval.

3. Accessibility and User Task Completion:

. Measure adherence to accessibility standards (e.g., WCAG).
a. Collect user input about accessibility features.
b. Measure the percentage of users who successfully complete a task on the first attempt.

4. Ongoing Improvement and Training:

. Monitor ongoing training and development for UI/UX designers.
a. Track the frequency of sessions aimed at improving design skills and collaboration.
b. Measure time dedicated to exploring new design trends and technologies.

H. STANDARD OPERATING PROCEDURE (SOP)

a. Purpose

To ensure efficient and consistent operations within the SADU, facilitating seamless software deployment and digital transformation.

b. Scope

This SOP applies to all staff members within the SADU, covering reporting, escalation procedures, job descriptions, lines of command, and responsibilities.

c. Responsibilities and Roles

1. Project Manager: Oversees projects, ensuring on-time delivery and adherence to budget.
2. Business Analyst: Gathers and validates requirements, ensures alignment with stakeholder needs.
3. Software Developer: Develops and maintains software solutions.
4. Quality Assurance/Systems Analyst: Tests software for defects and ensures quality standards.
5. System Administrator: Manages IT infrastructure and ensures system uptime.
6. Code Vulnerability Expert: Oversees security measures and compliance.
7. Process Analyst: Analyzes and improves business processes.
8. Support Engineer: Provides technical support and resolves issues.

Software and Applications Development Unit Head: Responsible for overall performance, meeting KPIs, and strategic alignment.

0. **All Staff:** Ensure timely completion of assigned tasks, adhere to security protocols, and maintain open communication within the team.

d. Reporting Procedure

1. Daily stand-up meetings for team updates with Unit Head.
2. Weekly progress reports submitted by each team member to the Project Manager/ Unit Head.
3. Monthly performance reviews conducted by the Director of COMSIT.

5. Escalation Procedure

1. Issues are first reported to the immediate supervisor.
2. If unresolved, the issue is escalated to the Unit Head.
3. Further escalation goes to the Director of COMSIT if necessary.

I. Lines of Command (top-down)

1. Director of COMSIT
2. Unit Head
3. Project Manager
4. Team Leads (Business Analyst, System Administrator, etc.)
5. Individual Contributors (Developers, QA Engineers, etc.)

J. Document control

1. Types of Documents:
   - Requirements Specifications
   - Design Documents

- Test Plans and Reports
- User Manuals
- Change Requests

2. Version Control System (tracking, back up, etc):
- Implement a version control system to manage document versions, changes, and collaboration.

3. Document Approval Process:
- Define a clear approval workflow for documents, including review cycles and sign-off procedures.

4. Access Control:
- Establish access permissions to ensure that only authorized personnel can view, edit, or approve documents.

5. Document Storage and Retrieval:
- Utilize a centralized document repository with a logical structure for easy storage, retrieval, and searchability.

K. FUTURE EXPANSION PLANS

1. New Technology Adoption:
Stay abreast of emerging technologies and trends to incorporate innovative solutions into development processes.
2. Capacity and Human Resource Development:
Invest in training programs to upskill team members and equip them with the latest tools and techniques.
3. Collaboration with Research Institutions:
Explore partnerships with research institutions to leverage cutting-edge research for new software development approaches.
4. International Collaboration:
Foster collaborations with international counterparts to exchange knowledge, best practices, and foster cross-cultural understanding.

L. Communication Plan

1. Internal Communication:
    1. Regular team meetings to discuss project updates, challenges, and achievements.
    2. Utilize collaboration tools (e.g. Microsoft Teams) for real-time communication and file sharing.
    3. Quarterly unit meetings to share updates and gather feedback from team members.

2. External Communication:

1. Establish a dedicated email address and contact point for external inquiries and feedback.
2. Maintain an active presence on social media platforms to showcase projects, achievements, and job opportunities.
3. Participate in industry events, conferences, and webinars to network and promote the unit's capabilities.

M. COMMUNICATION PROTOCOL

1. Email Communication:

1. -Use clear and concise language in email communication.
2. Include relevant subject lines and action items for quick reference.
3. Follow up on important emails to ensure timely responses.

2. Hard copy memoranda:

- Establish a standardized format for hard copy paper memos, including headings, date, recipients, sender's name, and signature fields, etc.

a. Distribution List:

Maintain an up-to-date distribution list for paper memos to ensure that the right individuals receive the information in a timely manner.

b. Tracking and Recording:

Implement a system for tracking and recording the distribution of paper memos, including acknowledgement of receipt and any follow-up actions required.

c. Enforce strict confidentiality measures for sensitive information included in paper memos, such as handling procedures and secure storage.

d. Archiving and Retention: Establish guidelines for the archiving and retention of paper memos, including storage duration and disposal procedures in compliance with data protection regulations.

e. Version Control: Maintain version control for paper memos by including a version number or date to ensure that the most recent information is being referenced.

3. Meeting Etiquette:

1. Start meetings on time and adhere to the agenda to maximize productivity.
2. Assign roles (e.g., facilitator, timekeeper) to ensure efficient meeting management.
3. Encourage active participation and respectful dialogue among team members.

4. Feedback Mechanisms:
    1. Implement regular feedback sessions to gather input on communication effectiveness and areas for improvement.
    2. Provide avenues for anonymous feedback to encourage candid responses.
    3. Act on feedback promptly to address concerns and enhance communication practices.

N. Interfacing areas with other COMSIT units:

- Collaborate with related units to ensure cohesive development and implementation strategies.

O. CONCLUSION

The SADU is poised to become a cornerstone of the University's digital strategy, enabling a culture of innovation and efficiency. Through strategic planning, careful resource management, and a commitment to continuous improvement, the SADU will contribute significantly to the University's reputation as a leader in sustainable digital transformation.

Software and Hardware Installation, Repair, and Maintenance Unit

COMPUTER SERVICES AND INFORMATION TECHNOLOGY (COMSIT) DIRECTORATE

A. OPERATIONAL BRIEF

The unit shall be responsible for in-house installation, repair and maintenance of computer software and hardware. The unit shall strive to contribute to the IGR of the University by providing essential services to members of the University's community at subsidized rates.

B. INTRODUCTION

The operations of the Software and Hardware Installation, Repair, and Maintenance (SHIRM) Unit, is a crucial component of COMSIT Directorate. The unit's core responsibilities include:

1. **Installation and Deployment:** Providing timely and efficient installation and deployment of all software and hardware systems across the university, ensuring compliance with university standards and security protocols.
2. **Repair and Maintenance:** Performing comprehensive repairs and maintenance of all university hardware and software assets. This includes proactive monitoring, scheduled maintenance procedures, and rapid response to reported faults, minimizing downtime and maximizing the lifespan of equipment.
3. **Troubleshooting and Support:** Providing first-line and escalated technical support to university users experiencing hardware or software issues. This encompasses detailed diagnostics, problem resolution, and user training to promote self-sufficiency.
4. **System Certification and Security:** Ensuring all systems meet established security standards and undergo regular audits for compliance. The unit is responsible for implementing and maintaining robust security protocols to protect sensitive data and prevent system breaches.
5. **ICT Asset Management:** Implementing and managing a comprehensive ICT asset tracking system in collaboration with the Bursary Stores Unit to monitor equipment lifecycle, inventory levels, and maintenance schedules, optimizing resource allocation and minimizing waste.
6. **Training and Skill Development:** Providing training and skills development programs for university staff and students, enhancing their understanding of technology and promoting best practices in equipment usage and maintenance. This includes formal training sessions, workshops, and readily accessible documentation.
7. **Revenue Generation:** Developing and implementing strategies to generate revenue through service contracts with internal departments and external clients, while ensuring cost-effectiveness and service quality. This contributes to the unit's self-sustainability and reduces its reliance on university funding.

C. MISSION STATEMENT:

To deliver efficient and reliable technical support for software and hardware systems, ensuring minimal downtime and maximizing productivity across the university community, while fostering student skill development and contributing to the institution's self-sufficiency.

D. **STAFFING**

The SHIRM unit has the following:

1. **Head of Unit:** Oversees all aspects of the unit, sets strategic direction, and ensures adherence to university policies and best practices.
2. **Team Leads:** Each leads a specialized team (e.g., Hardware Maintenance, Software Maintenance, Training and Support).
3. **Technicians:** Perform hands-on repair and maintenance tasks, categorized based on expertise (e.g., desktop support, server administration, network technician).
4. **Administrative Staff :** Handles scheduling, billing, inventory management, and client communication.

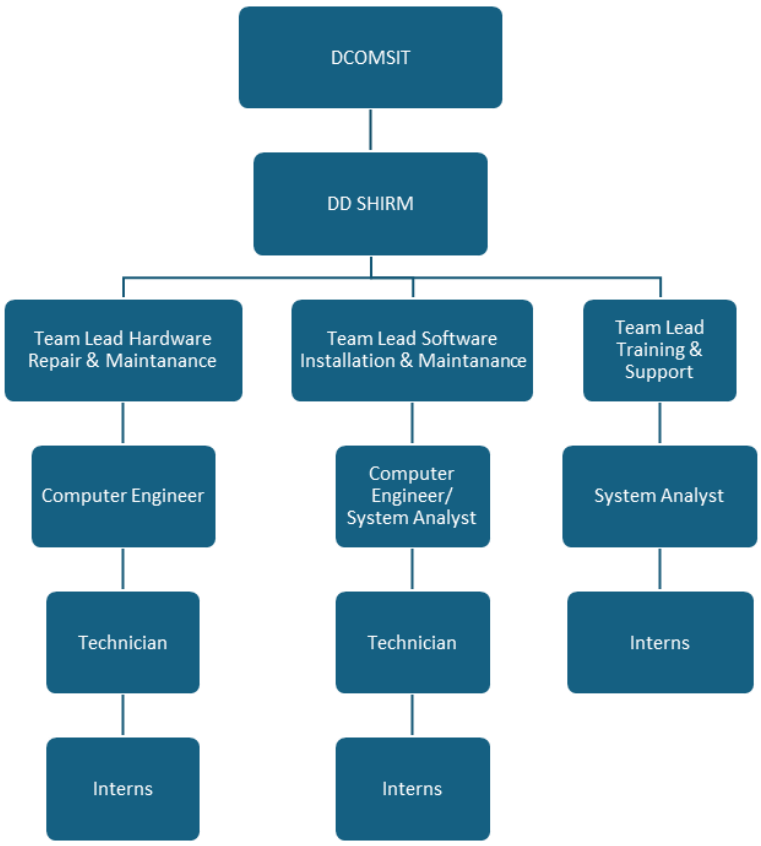
II. Job Descriptions:

Head of Unit:

1. Reports to: COMSIT Director
2. Responsibilities: Overall strategic direction, budget management, performance review, stakeholder relations, policy compliance.
3. **Team Leads:** (Each reports directly to the Unit Head/Manager)
4. **Team Lead – Hardware Maintenance:** Manages hardware technicians; responsible for hardware repair, maintenance, inventory.
5. **Team Lead – Software Maintenance:** Manages software technicians; responsible for software installation, updates, troubleshooting.
6. **Team Lead – Network Infrastructure:** Manages network technicians; responsible for network maintenance, security, and troubleshooting.
7. **Team Lead – Training and Support:** Manages support staff and interns; responsible for user training, help desk operations, documentation.
8. **Technicians:** (Each reports to their respective Team Lead)
9. Several technicians under each Team Lead, specialized by area (e.g., Desktop Support Technicians, Server Administrators, Network Technicians).

Student Interns: (Report to their respective Team Lead)
Administrative Staff: (Reports directly to the Unit Head)

E. UNIT ORGANOGRAM



Line of Reporting:

All staff members report to their immediate supervisor. The chain of command flows from the technicians and interns to their team leads, and then from the team leads to the Unit Head/Manager. The Unit Head/Manager, in turn, reports to the COMSIT Director.

F. **SWOT ANALYSIS**

This SWOT analysis evaluates University of Ilorin's Software and Hardware Installation, Repair, and Maintenance (SHIRM) unit.

I. Strengths:

1. **Existing Technical Expertise:** The unit possesses a foundation of technical expertise within its staff, offering a valuable starting point for enhanced service delivery and innovation. This is a key asset that can be further developed through training and strategic recruitment.
2. **Potential for Collaboration:** The SHIRM unit is well-positioned to collaborate effectively with other COMSIT units (NOC, Software Development, Cybersecurity, etc.).
3. **Student Internship Program:** The proposed internship programme will provide access to a readily available pool of students. This allows for cost-effective project completion,

practical training for students, and a source of human resources for future hires within the unit.

4. **Revenue Generation Potential:** from both within and outside the university community. This fund is sourced from internal service fees (subsidised), external clients, and specialized training programs.

II. Weaknesses:

1. **Staffing Uncertainty and Resource Constraints:** The unit acknowledges initial challenges in forecasting staffing needs and securing adequate resources. Addressing this is critical for sustained growth and the ability to handle increasing workloads. A detailed staffing plan with clear skill requirements and a competitive compensation strategy is essential.
2. **Limited Brand Recognition:** The unit currently lacks significant brand recognition externally. A focused marketing campaign is needed to establish its reputation for quality service and attract external clients.
3. **Performance Measurement Gaps:** The absence of established Key Performance Indicators (KPIs) hinders effective performance tracking and continuous improvement. Clear, measurable KPIs are needed across service delivery, efficiency, and client satisfaction.
4. **Dependency on External Vendors:** Reliance on external vendors for specialized repairs creates potential delays and cost inefficiencies. Developing internal expertise in specialized areas or establishing strategic partnerships could mitigate this weakness.
5. **Infrastructure Limitations:** Inadequate diagnostic tools and software licenses may limit the unit's ability to handle advanced repairs and offer a wider range of services. Investing in updated infrastructure is crucial for remaining competitive.

III. Opportunities:

1. **Expanding Service Offerings:** The market demands a wider range of IT services. The unit can capitalize on this by adding advanced services like data recovery, cloud solutions, cybersecurity consulting, and specialized training programs.
2. **Strategic Partnerships:** Collaborating with external tech companies (vendors, distributors) can secure discounted pricing on hardware and software, open avenues for joint ventures, and expand the unit's service capabilities.
3. **Targeting External Clients:** Aggressive marketing campaigns focused on local businesses, government agencies, and NGOs can significantly increase revenue streams and contribute to self-sustainability.
4. **Leveraging Technology Advancements:** Adopting emerging technologies (AI, automation) will enhance service efficiency, reduce labor costs, and improve service quality.

5. **Strengthening Community Engagement:** Offering specialized workshops and training programs to the local community can enhance the unit's reputation and create additional revenue streams.

IV. Threats:

1. **Competition from Private IT Service Providers:** The unit faces competition from established private IT companies with established reputations and rapid response times. Differentiation through superior service quality, competitive pricing, and a strong brand identity are crucial.
2. **Rapid Technological Change:** The fast-paced evolution of technology necessitates ongoing staff training and investment in the latest tools and technologies to maintain competitiveness.
3. **Budget Constraints:** University-wide financial limitations could restrict resource allocation and hinder growth. Effective budget management and demonstrating a strong ROI are essential.
4. **Market Saturation:** An already crowded market requires a strong marketing strategy to carve out a niche and attract a significant client base.
5. **Cybersecurity Risks:** Data breaches can severely damage the unit's reputation and incur significant costs. Investing in robust security measures and maintaining rigorous security protocols are crucial.

G. KEY PERFORMANCE INDICATORS (KPIs)

Service Delivery KPIs:

1. **Average Resolution Time (ART):** The average time taken to resolve a reported incident or service request. Target: Reduce ART by X% within Y months. (Specific, Measurable, Achievable, Relevant, Time-bound)
2. **Customer Satisfaction Score (CSAT):** Measured through surveys or feedback forms after service completion. Target: Achieve a CSAT score of X% or higher within Y months. (Specific, Measurable, Achievable, Relevant, Time-bound)
3. **First Call Resolution (FCR):** Percentage of incidents resolved on the first contact. Target: Achieve an FCR rate of X% or higher within Y months. (Specific, Measurable, Achievable, Relevant, Time-bound)
4. **Mean Time To Repair (MTTR):** Average time taken to restore a failed system or piece of equipment to operational status. Target: Reduce MTTR by X% within Y months. (Specific, Measurable, Achievable, Relevant, Time-bound)
5. **Mean Time Between Failures (MTBF):** Average time between failures of equipment or systems. Target: Increase MTBF by X% within Y years. (Specific, Measurable, Achievable, Relevant, Time-bound)

6. **Downtime Percentage:** Percentage of time systems or equipment are unavailable. Target: Reduce downtime percentage by X% within Y months. (Specific, Measurable, Achievable, Relevant, Time-bound)
7. **Service Level Agreement (SLA) Adherence:** The percentage of SLAs met with clients. Target: Achieve X% SLA adherence within Y months. (Specific, Measurable, Achievable, Relevant, Time-bound)

II. Financial KPIs:

1. **Revenue Generated:** Total revenue generated from internal service fees and external contracts. Target: Increase revenue by X% within Y years. (Specific, Measurable, Achievable, Relevant, Time-bound)
2. **Cost per Incident:** The average cost of resolving a single incident. Target: Reduce cost per incident by X% within Y months. (Specific, Measurable, Achievable, Relevant, Time-bound)
3. **Profit Margin:** The unit's profit margin on services provided. Target: Achieve/maintain a profit margin of X% within Y years. (Specific, Measurable, Achievable, Relevant, Time-bound)
4. **Return on Investment (ROI) of Training Programs:** Measure the financial return generated from specialized training programs. Target: Achieve an ROI of X% or higher within Y years for each training program. (Specific, Measurable, Achievable, Relevant, Time-bound)

III. Operational Efficiency KPIs:

1. **Inventory Turnover Rate:** Measure how efficiently the unit manages its inventory of parts. Target: Maintain an inventory turnover rate of X times per year. (Specific, Measurable, Achievable, Relevant, Time-bound)
2. **Ticket Closure Rate:** The number of tickets closed versus opened per period. Target: Maintain a closure rate exceeding X% per month. (Specific, Measurable, Achievable, Relevant, Time-bound)
3. **Number of Preventive Maintenance Tasks Completed:** Tracking the number of preventative maintenance tasks completed per period. Target: Complete X number of preventive maintenance tasks per month. (Specific, Measurable, Achievable, Relevant, Time-bound)
4.

IV. Innovation and Skill Development KPIs:

1. **Number of New Services Introduced:** Track the introduction of new services or solutions. Target: Introduce X new services within Y years. (Specific, Measurable, Achievable, Relevant, Time-bound)
2. **Employee Training Hours:** Total hours of training completed by staff per period. Target: Each staff member completes X hours of training per year. (Specific, Measurable, Achievable, Relevant, Time-bound)
3. **Student Internship Success Rate:** Percentage of student interns who successfully complete their internships. Target: Achieve an internship success rate of X% or higher within Y years. (Specific, Measurable, Achievable, Relevant, Time-bound)

V. Data Collection and Reporting:

Implementing these KPIs requires a robust system for data collection and reporting. This include a ticketing system, customer feedback mechanisms, and regular performance reviews. The data would be analyzed regularly to track progress, identify areas for improvement, and inform strategic decision-making. Using a dedicated dashboard for visualizing these KPIs will be highly beneficial.

H. STANDARD OPERATING PROCEDURE (SOP)

I. Purpose: This SOP outlines the standardized workflows, responsibilities, and escalation procedures for the Software and Hardware Installation, Repair, and Maintenance (SHIRM) unit, ensuring consistent, high-quality service delivery aligned with global best practices in world-class universities.

II. Scope: This SOP applies to all staff within the SHIRM unit, including the Unit Head/Manager, Team Leads, Technicians, and Student Interns, covering all aspects of service delivery from initial request to completion and follow-up.

III. Structure of Operations:

The SHIRM unit operates under a hierarchical structure with clearly defined roles and responsibilities:

1. **Head of Umit:** Oversees all operations, ensuring adherence to this SOP, managing resources, and reporting to the COMSIT Director.
2. **Team Leads (Hardware, Software, Network, Training & Support):** Manage their respective teams, delegate tasks, and ensure timely completion of work.
3. **Technicians:** Perform hands-on installations, repairs, and maintenance tasks according to established procedures.
4. **Interns:** Assist technicians under close supervision.
5. **Administrative Staff:** Manage scheduling, billing, inventory, and client communication.

IV. Responsibilities:

1. **Unit Head/Manager:** Strategic planning, resource allocation, budget management, performance monitoring, compliance, stakeholder communication, staff training.
2. **Team Leads:** Team management, task delegation, quality control, technical guidance, training, escalation of complex issues.
3. **Technicians:** Execute repairs, installations, and maintenance tasks based on established procedures; document all work accurately; escalate problems to Team Leads as needed.
4. **Interns:** Assist technicians; learn established processes and procedures; work under direct supervision.
5. **Administrative Staff:** Maintain accurate records, handle client communication, manage inventory, process billing, prepairs reports.

V. Job Descriptions: (Detailed job descriptions for each role should be created as separate documents, referencing this SOP.)

VI. Service Request Process:

1. **Request Submission:** Clients (internal or external) submit service requests through an established ticketing system. The system should capture all relevant details (equipment type, problem description, contact information, etc.).
2. **Ticket Assignment:** The administrative staff assigns tickets to the appropriate team lead based on the nature of the request.
3. **Initial Assessment:** The Team Lead assesses the request, determines the necessary actions, and assigns tasks to technicians or interns.
4. **Service Delivery:** Technicians perform the required work following established procedures. All work is documented in the ticketing system, including steps taken, parts used, and time spent.
5. **Quality Control:** The Team Lead reviews the completed work, ensuring compliance with quality standards and documenting outcomes.
6. **Client Communication:** Administrative staff updates the client on the progress and completion of the service request.
7. **Closure:** Once the client confirms satisfaction, the ticket is closed.

VII. Escalation Procedure:

1. Technicians escalate complex or unresolved issues to their Team Lead.
2. Team Leads escalate issues beyond their expertise or involving significant resources to the Unit Head/Manager.
3. The Unit Head/Manager escalates issues involving multiple units or requiring significant budgetary approval to the COMSIT Director.

VIII. Line of Reporting:

1. All staff report to their immediate supervisor. The hierarchy is: Technicians/Interns → Team Leads → Unit Head/Manager → COMSIT Director.

IX. Global Standard Practice Alignment:

This SOP aligns with global best practices in university IT service management by emphasizing:

1. **ITIL Framework:** Integration of ITIL principles for efficient service management.
2. **ISO Standards:** Compliance with relevant ISO standards for IT service management.
3. **Customer Focus:** Prioritizing customer satisfaction through timely and effective service delivery.
4. **Continuous Improvement:** Regular review and updates to the SOP based on performance data and feedback.
5. **Knowledge Management:** Creating and maintaining a comprehensive knowledge base for efficient problem-solving.
6. **Risk Management:** Identifying and mitigating potential risks to service delivery.
7. **Security Protocols:** Maintaining the highest security standards throughout all procedures.

X. Documentation and Review:

This SOP will be regularly reviewed and updated (at least annually) by the Unit Head/Manager, ensuring it remains current, relevant, and effective. All work performed under this SOP must be meticulously documented.

XI. Training:

All SHIRM unit staff will receive comprehensive training on this SOP and any updates. Ongoing training on relevant technologies and service management best practices will be ensured.

This detailed SOP provides a robust framework for the SHIRM unit. Remember to add specific details on tools, technologies, and internal processes used within the unit for a fully functional document. Regular training and review are crucial for sustained compliance and improvement.

Document Control: The SHIRM unit will maintain a central repository for all SOPs and related documentation. Each document will have a unique identifier (e.g., document number, version number, revision date). A version control system will track all changes and revisions, ensuring that only the most up-to-date version is used. A document change log will record who made the change, when it was made, and the reason for the change.

Document Approval Process: All SOPs and other controlled documents will undergo a formal approval process. This process will typically involve review and approval by the relevant Team Lead, the Unit Head/Manager, and potentially the COMSIT Director, depending on the document's scope and impact. Approval signatures and dates will be recorded on each document.

Access Control: Access to SOPs and related documents will be controlled to ensure that only authorized personnel can view and/or modify them. Access levels will be assigned based on roles

and responsibilities within the unit. A password-protected electronic document management system will be used for secure storage and retrieval.

Document Storage and Retrieval: All SOPs and controlled documents will be stored securely in both electronic and physical formats. The electronic storage system will allow for easy retrieval and version control. Physical copies will be stored in a secure, controlled environment. A clear system for document retrieval will be established, including an easily searchable electronic index and a physical filing system. Regular audits will ensure compliance with storage and retention policies.

Future Expansion Plan for the SHIRM Unit:

The SHIRM unit's future expansion should be guided by a strategic plan focusing on several key areas:

1. **Service Diversification:** Expand service offerings to include higher-value services like advanced data recovery, cloud computing solutions, cybersecurity assessments and consulting, and specialized software development. This will attract a broader client base and increase revenue.
2. **Market Penetration:** Actively target external clients through a comprehensive marketing campaign, including social media marketing, attending industry events, and building relationships with local businesses, government agencies, and NGOs. This will raise the unit's profile and increase external contract opportunities.
3. **Strategic Partnerships:** Forge strategic alliances with major technology companies (hardware and software vendors) to become certified service providers. This will unlock discounted pricing, access to training and support, and potentially joint ventures to offer comprehensive solutions.
4. **Technology Integration:** Invest in automation tools and AI-driven diagnostic capabilities. This will enhance service efficiency, reduce turnaround times, and improve the accuracy of repairs. Advanced diagnostic tools will allow the unit to handle more complex issues.
5. **Enhanced Internship Program:** Expand the internship program to involve a larger number of students, providing hands-on experience and developing a skilled workforce pipeline for the future.
6. **Specialized Training Workshops:** Develop and deliver specialized training workshops on current IT trends to generate additional revenue and enhance community skills. These workshops could be open to both internal and external participants.
7. **Financial Sustainability:** Implement a robust system for internal service fees to ensure prompt service and generate funds for the unit. Explore opportunities to license proprietary software solutions developed internally to other universities or organizations.

Communication Plan:

The communication plan should ensure effective information flow among the SHIRM team, other COMSIT units, and external stakeholders.

1. **Internal Communication:** Regular bi-weekly team meetings will be held to discuss progress, challenges, and upcoming projects. A dedicated communication channel (e.g., internal messaging platform) will facilitate rapid information sharing. A suggestion box will allow staff to propose improvements.
2. **External Communication:** A comprehensive marketing campaign will be launched targeting potential clients. This will include regular newsletters to update stakeholders on unit achievements and upcoming services. A website and social media presence will be established. Regular communication with external partners will maintain positive relationships and facilitate collaboration.
3. **Feedback Mechanism:** Establish a formal feedback mechanism, allowing clients (internal and external) to provide input on service quality and suggest improvements. This feedback will be used to continuously improve service delivery and update SOPs.

Communication Protocol:

The SHIRM unit should use a clear and consistent communication protocol to ensure effective information exchange.

1. **Ticketing System:** All service requests and communications will be managed through a central ticketing system, ensuring accountability, tracking progress, and providing a clear audit trail.
2. **Email Communication:** Formal communication with external clients and stakeholders will be primarily through email, using a professional and consistent tone.
3. **Reporting:** Regular reports will be generated for the COMSIT Director, highlighting key performance indicators (KPIs), progress towards goals, and any challenges encountered.
4. **Emergency Communication:** Establish a clear protocol for emergency communication, ensuring rapid response to critical incidents and minimizing downtime.
5. **Meeting Procedures:** Develop standard procedures for meetings, including agendas, meeting minutes, and action items.

By implementing these plans and protocols, the SHIRM unit can foster effective communication and collaboration, leading to improved efficiency, enhanced service delivery, and successful expansion. Remember to tailor the plans to the specific context of the University of Ilorin and its resources.

The Software and Hardware Installation, Repair, and Maintenance (SHIRM) unit at the University of Ilorin should play a collaborative and strategic role within the COMSIT directorate and the wider university community. This can be achieved through well-defined interfaces and processes that foster seamless information exchange, efficient resource allocation, and

synergistic service delivery. Here's a breakdown of how the SHIRM unit can interface with other COMSIT units and the university community:

I. INTERFACING AREAS WITH OTHER COMSIT UNITS AND THE UNIVERSITY COMMUNITY

J. . Interfaces with Other COMSIT Units:

The SHIRM unit's success hinges on strong collaboration with other COMSIT units. Strategic interfaces would be established to streamline workflows and leverage expertise across the directorate:

1. **Administration and Operations:** The SHIRM unit will collaborate with Administration and Operations on standardizing administrative procedures (service requests, billing, reporting) and resource allocation strategies for efficient personnel and technology use. This includes coordinating budget requests and reporting financial data.
2. **Network Operations Center (NOC):** Close coordination with the NOC is crucial for ensuring optimal network infrastructure performance. The SHIRM unit should jointly develop incident response protocols for network issues requiring hardware or software intervention. This might involve joint training to ensure both teams understand each other's procedures.
3. **Software Development:** The SHIRM unit will partner with Software Development to ensure newly developed applications are correctly installed and maintained. The SHIRM unit will provide feedback on hardware performance to inform software development, enhancing compatibility and user experience. This is essential for the smooth operation of university systems.
4. **Cybersecurity and Multimedia:** The SHIRM unit will work closely with Cybersecurity to ensure that all software installations comply with university security protocols. The SHIRM unit will promptly report any security incidents detected during repairs or installations. This joint effort will safeguard the university's IT infrastructure.The SHIRM unit will collaborate on maintaining multimedia equipment. They can jointly conduct workshops to educate staff and students on using multimedia tools effectively.
5. **Mail Services and Help Desk:** The SHIRM unit will coordinate with Help Desk to resolve user-reported issues efficiently. This may involve joint training to help the Help Desk staff effectively triage and escalate issues to the SHIRM unit.
6. **Training:** The SHIRM unit will collaborate with Training to develop joint internship programs, providing hands-on experience for students and developing a skilled workforce for the future. Joint training sessions covering hardware maintenance, software applications, and other relevant IT areas can be offered to university staff.
7. **IT Ideation and Innovation:** The SHIRM unit will share findings from repairs and maintenance activities to inform innovation initiatives, contributing to proactive IT strategies.

8. **Research and Development (R&D):** Joint research projects focusing on emerging technologies relevant to hardware maintenance and software installation can be undertaken. This collaboration would enhance the unit's expertise and contribute to the university's research output.

K. INTERFACE WITH THE UNIVERSITY COMMUNITY:

The SHIRM unit's success requires a strong interface with the university community:

1. **Internal Departments and Faculties:** The unit will provide cost-effective IT services to internal departments and faculties. They will use a service level agreement (SLA) system to clearly define service expectations and ensure prompt service delivery.
2. **External Clients:** The unit will actively market its services to local businesses, government agencies, and NGOs. They will establish service contracts, offering various service packages tailored to client needs. A robust communication and feedback system will be implemented to ensure client satisfaction.
3. **Student Engagement:** The unit will leverage student interns to enhance its operational efficiency and provide valuable practical experience for students. Regular feedback will be collected from interns to enhance the internship program.

By implementing these collaborative interfaces and processes, the SHIRM unit can effectively leverage the resources and expertise within the COMSIT directorate, serving the university community efficiently and effectively while contributing significantly to its financial health and technological advancement.

O. Conclusion:

The establishment of a robust and efficient SHIRM unit is a strategic imperative for the University of Ilorin. This blueprint provides a clear roadmap for achieving operational excellence, financial sustainability, and impactful contributions to the university community. By leveraging existing strengths and addressing identified weaknesses, the SHIRM unit is well-positioned to not only meet the university’s IT needs but also to become a leading provider of IT services in the region. The integration of student internships enhances practical training opportunities, fostering a skilled workforce while contributing to cost-effective operations. This proactive, innovative, and collaborative approach ensures the SHIRM unit will remain adaptable, responsive, and competitive, securing its position as a valuable asset for the university for years to come. The successful implementation of this blueprint will not only enhance the technological infrastructure of the University but also serve as a model for other units within COMSIT and beyond, demonstrating the potential for self-sustaining and impactful operations within a higher education environment.

Training Unit

COMPUTER SERVICES AND INFORMATION TECHNOLOGY (COMSIT) DIRECTORATE

A. OPERATIONAL BRIEF

The unit shall be responsible for coordinating all ICT trainings and certifications within the University including hands-on trainings on automated processes of the University in line with global best practices. The unit shall equally drive the new innovative ICT short courses in conjunction with the university's consultancy unit.

B. INTRODUCTION:

The Training Unit of COMSIT Directorate is primarily responsible for equipping the university community and general public with the necessary ICT skills and knowledge for effective service delivery. This involves a broad spectrum of activities, including:

1. **Needs Assessment:** Identifying the ICT training requirements of different faculties, departments, units or individuals based on their roles and responsibilities.
2. **Training Program Development:** Designing and developing ICT training programmes, workshops, and courses aligned with the identified needs.
3. **Training Delivery:** Conducting training sessions, workshops, and webinars using various methods (classroom, online, or blended learning).

C. MISSION STATEMENT

The training unit is established for the purpose of empowering university workforce and other members of the public with necessary ICT skills and knowledge to enhance productivity, innovation, and overall organizational performance.

D. STAFFING:

The roles in the Training Unit are as specified:

1. **Head of Unit/Training Manager (1):** Oversees the operations of the unit ranging from planning, designing and execution of training activities and other oversight functions.
2. **Facilitators** (Indefinite - to be outsourced both locally and outside the university):

i. Deliver training courses on various ICT topics (e.g., software applications, hardware, networking, cybersecurity, project management etc.

ii. Develop training materials and resources.

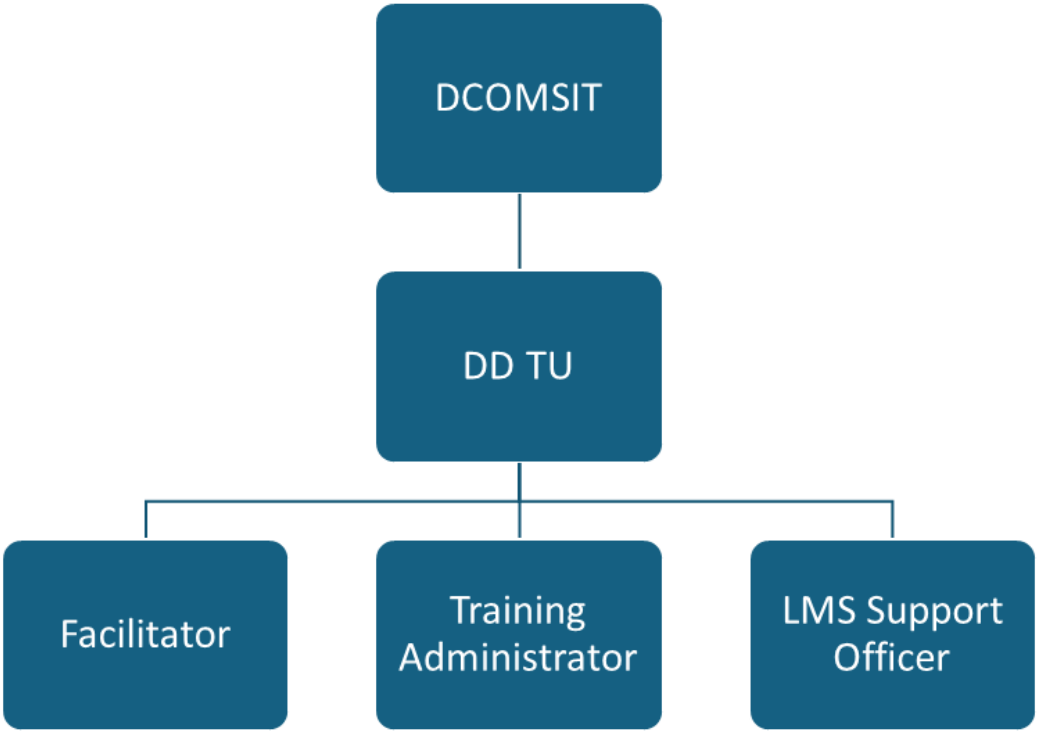
iii. Provide technical support to trainees.

iv. Conduct training needs assessments.

0. **Training Administrator(1):**

   i. Handles training logistics (scheduling, room booking, equipment)
   ii. Manages trainee records and certifications.
   iii. Provides administrative support to the training team
0. **Learning Management System (LMS) Support Officer (1):**
   i. Manages the unit's LMS platform.
   ii. Develops and uploads training content.
   iii Provides technical support for LMS users.

E. UNIT ORGANOGRAM



F. **SWOT Analysis**

Strengths:

1. **Expertise:** Availability of resourceful personnel who have adequate skills and relevant certifications in diverse areas of ICTs. The University is equally endowed with relevant experts in pedagogy and curriculum development capable of facilitating development of quality training materials.
2. **Flexibility**: There is a possibility of varying delivery strategy depending on the specific needs of the target audience.

3. **Weaknesses:**

1. Limited resources for developing specialized training content.
2. Potential challenges in balancing the demands of university students and external participants.
3. Inadequate funding

Opportunities:

1. Expansion of training offerings to cater for emerging technologies and market demand.
2. Collaboration with industry partners to enhance the relevance of training need and then tailor some customized programs to enable wider clients.

Threats:

1. Competition from other training providers offering similar programs.
2. Difficulty in attracting participants due to completive training schools that have littered all over

G. KEY PERFORMANCE INDICATORS (KPIs).

1. Number of participants enrolled in training programmes over a period f time
2. Participant's satisfaction ratings of training delivered over a period of time.
3. Employment placement rating of program graduates over a period of time.
4. Number of industry partnerships established and job placement opportunities over a period of time.

H. Standard Operating Procedure (SOP)

A Standard Operating Procedure (SOP) for training outlines the steps and guidelines for conducting effective training sessions. Here's a general template:

I. Pre-Training Preparation

1. Define training objectives and outcomes
2. Identify target audience and their needs
3. Develop training content and materials
4. Schedule training sessions and logistics
5. Notify participants and stakeholders

II. Training Delivery

1. Introduce training objectives and agenda

2. Deliver training content using various methods (e.g., lectures, discussions, hands-on exercises)
3. Encourage participant engagement and feedback
4. Provide opportunities for questions and answers
5. Monitor and adjust training pace as needed

III. Training Evaluation

1. Distribute evaluation forms to participants
2. Collect feedback and suggestions for improvement
3. Assess participant understanding and knowledge retention
4. Identify areas for improvement and implement changes
5. Document evaluation results and recommendations

IV. Post-Training Activities

1. Provide additional resources and support
2. Encourage participants to apply new skills and knowledge
3. Monitor and evaluate training effectiveness
4. Recognize and reward participants' achievements
5. Review and revise training content and materials as needed

V. Training Documentation

1. Maintain training records and documentation
2. Store training materials and resources
3. Update training manuals and guides
4. Share training best practices and lessons learned
5. Review and revise SOPs as needed

This SOP template provides a general framework for conducting training sessions. You can customize it to fit your organization's specific needs and requirements.

Procedures in which you carry out operations in your unit. E.g. reporting, escalation, job description, line of command, responsibilities, etc.

I. LINE OF COMMAND

1. Director of COMSIT
2. Unit Head

3. Facilitator
4. Training Administrator
5. LMS Support Officer

J. DOCUMENT CONTROL

1. **Version Control**: Keep track of different versions of the document to ensure everyone is using the most up-to-date version.
2. **Storage and Retrieval**: Organize and categorize documents in a clear structure, using appropriate naming conventions and directories.
3. **Security**: Implement access controls, passwords, encryption, and user permissions to prevent unauthorized access and modifications.
4. **Reviews and Approvals**: Establish review processes to ensure documents are checked for correctness, policy conformance, and regulatory compliance before they are shared.
5. **Unique Identification**: Assign unique identification numbers or codes to track documents easily and prevent outdated versions from being used.
6. **Distribution:** Use email notifications or cloud-based sharing platforms to share documents, ensuring everyone has the latest information.
7. **Retention and Archiving**: Establish guidelines for how long documents should be kept before archiving or destroying them, ensuring they meet legal requirements.
8. **Document Control Team**: Have a dedicated team responsible for managing document control processes and ensuring compliance with established policies and procedures

J. FUTURE EXPANSION

The future expansion of an ICT Directorate's training unit is contingent on several factors, including the organization's strategic goals, technological advancements, and the evolving needs of the workforce. Here are some key areas to consider for expansion:

Identifying Expansion Needs

1. **Needs Assessment:** Conduct a thorough assessment of the current training programs, identifying gaps, inefficiencies, and areas for improvement.
2. **Strategic Alignment:** Ensure that training aligns with the organization's overall strategic objectives and business goals.
3. **Technology Audit:** Analyze the latest technological trends and their impact on the workforce, determining the necessary training requirements.
4. **Skill Gap Analysis:** Identify the specific skills and competencies required for future roles and responsibilities.

Expansion Areas

1. **Curriculum Development:**

    1. Expand training offerings to cover emerging technologies and digital skills (e.g., AI, cloud computing, cybersecurity, data analytics).
    2. Develop specialized training programs for different departments or roles within the organization.
    3. Create modular training programs to allow for flexibility and customization.

2. **Training Delivery Methods:**

    1. Explore blended learning approaches combining classroom instruction, online learning, and hands-on practice.
    2. Utilize e-learning platforms and digital tools for efficient knowledge transfer.
    3. Offer self-paced learning options to accommodate diverse learning styles and schedules.

3. **Training Infrastructure:**

    1. Upgrade training facilities with modern equipment and technology.
    2. Expand training capacity to accommodate a larger number of participants.
    3. Develop a robust Learning Management System (LMS) to track training progress and performance.

4. **Trainer Development:**

    1. Invest in the professional development of training staff to enhance their skills and knowledge.
    2. Provide opportunities for trainers to specialize in specific areas of expertise.
    3. Encourage the adoption of innovative teaching methodologies.

5. **Performance Measurement and Evaluation:**

    1. Implement a comprehensive evaluation system to measure the effectiveness of training programs.
    2. Track training outcomes and their impact on employee performance and organizational goals.
    3. Use data-driven insights to inform future training initiatives.

K. COMMUNICATION PLANS

L. **Communication Protocol:** email, phone calls and physical meeting.

1. Internal Communication: meeting, email, etc.
2. External Communication: email, phone call, physical meetings, etc

N. INTERFACING AREAS WITH OTHER COMSIT UNIT

A collaboration between the training unit and other units of the directorate is encouraged to achieve expected synergy of all interrelated processes.

O. CONCLUSION

The Training Unit (TU) is committed to providing emerging ICT skills and knowledge for individuals within the university and the extended community. By leveraging its strengths in curriculum design, experienced trainers, and industry partnerships, TU aims to become a hub for lifelong ICT learning and skills development. Through strategic planning, resource allocation, and continuous evaluation, TU will play a vital role in shaping the future workforce and contributing to the digital transformation of individuals and organizations.

Web Services Unit

A. OPERATIONAL BRIEF

The unit shall be responsible for planning, designing and managing the University's main website, sub-domains and other web services to achieve desired visibility and ranking.

B. INTRODUCTION

The University of Ilorin's Web Services (WS) Unit plays a pivotal role in enhancing the institution's digital presence. Its core mandate is the planning, design, management, and optimization of the university's web platforms including the main website, subdomains, and other web services to ensure visibility, scalability, security, and alignment with global best practices in higher education. This involves acting as a crucial interface between the university and its internal and external stakeholders, facilitating communication and information dissemination. The unit strives to establish a robust digital gateway that not only meets user needs but also adheres to international standards for web services, prioritizing user experience and security protocol compliance. The ultimate goal is to achieve a high ranking and prominent web presence for the university.

C. MISSION STATEMENT

To drive a sustainable globally competitive university web presence by providing a secure, scalable, and user-friendly web platform that fosters effective communication, enhances visibility, and supports the university's mission.

D. STAFFING

This staffing structure overviews comprehensive coverage of all aspects of the Web Services Unit's responsibilities.

I. Leadership and Coordination:

Head of Unit: oversees all aspects of the Web Services Unit, ensuring alignment with university goals and global best practices. Responsibilities include strategic planning, resource allocation, budget, performance monitoring, and staff supervision.

II. Web Development:

2. **Lead Web Developer (Webmaster):** Leads the development team, defining architecture, overseeing coding standards, and ensuring seamless integration across various technology stacks (REST, SOAP). Requires extensive experience in leading web development projects and managing teams.
3. **Senior Web Developers :** Experienced developers responsible for the design, coding, testing, and implementation of complex web applications. Expertise in front-end (HTML, CSS, JavaScript, React, Angular, Vue.js) and back-end (PHP, Python, Node.js, Java, .NET) development is needed.

4. **Junior Web Developers:** Develop and maintain website features under the guidance of senior developers.

III. User Experience (UX) and Design:

1. **UX Designer:** Designs and implements intuitive and user-friendly interfaces, improving user experience and engagement.
2. **UI/UX Designer (1):** Translate design concepts into functional web pages.

IV. Quality Assurance and Testing:

1. **Quality Assurance Expert:** Develops and executes comprehensive testing strategies to ensure web application quality, stability, and security. Experience in various testing methodologies (unit, integration, system, user acceptance testing) is essential.

V. Data Analytics and Performance Monitoring:

0. **Data Analyst:** Collects, analyzes, and interprets web analytics data to inform strategic decisions and improve website performance.

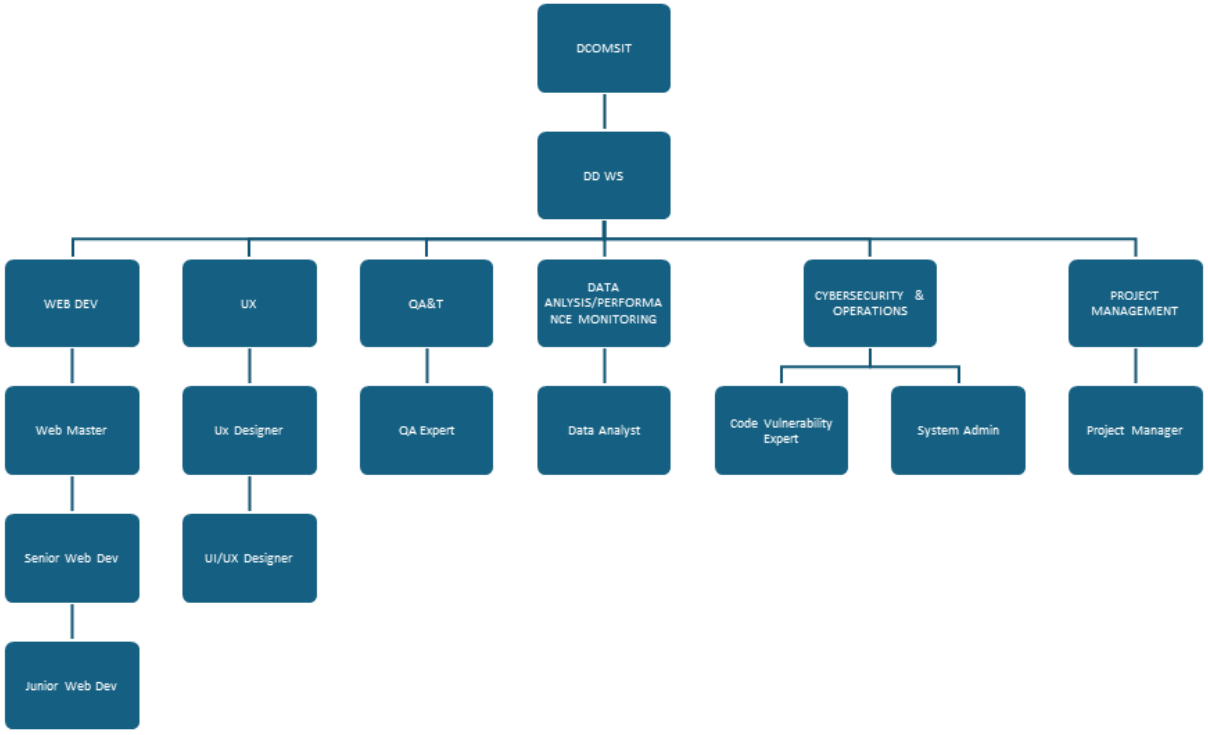
VI. Cybersecurity and Operations:

0. **Code Vulnerability Expert:** Implements and maintains security protocols (SSL/TLS, OAuth, OpenID Connect) to protect web applications from cyber threats. Experience in security auditing and incident response is critical. This person is responsible for security updates and ensuring compliance with relevant regulations.
1. **System Administrator:** Responsible for the day-to-day maintenance and management of web servers, databases, and related infrastructure.

VII. Project Management:

1. **Project Manager:** Manages web development projects, ensuring they are delivered on time, within budget, and to the required quality standards.

E. UNIT ORGANOGRAM



F. SWOT ANALYSIS

This SWOT analysis provides a comprehensive overview of the state of the Web Services Unit.

I. Strengths:

1. **Existing Skilled Personnel:** The unit has a core team of experienced web developers.
2. **Established Infrastructure:** The unit possesses existing infrastructure and processes for managing the university's web presence. This provides a solid foundation for building upon and enhancing services.
3. **Industry Standard Adherence:** The utilization of established protocols (REST, SOAP) and security measures (SSL/TLS, OAuth) ensures seamless integration and robust security, in line with global best practices and standards.
4. **Scalability:** The current system is designed to handle a large number of simultaneous requests, ensuring reliable performance even during peak usage. This is crucial for a large university.
5. **Interoperability:** The unit's systems are designed for communication between various software applications, allowing for the development of complex, scalable systems. This supports future expansion and integration with other university systems.

II. Weaknesses:

1. **Staffing Gaps:** The current team lacks UX/UI designers and data analysts, hindering the optimization of user experience and data-driven decision-making.

2. **Dependence on Connectivity:** The unit's effectiveness is dependent on a stable internet connection, which may pose challenges in areas with unreliable infrastructure. This vulnerability requires mitigation strategies.
3. **Complex Development Processes:** The development and maintenance of web services can be complex, leading to increased costs and time investment. Streamlining these processes is key.
4. **Limited Cybersecurity Expertise:** While security protocols are in place, dedicated cybersecurity expertise may be limited, leaving the unit vulnerable to evolving cyber threats. This requires additional personnel or external partnerships.
5. **Outdated Technology:** The unit may not fully utilize the latest technologies and frameworks. A technology audit and plan for upgrades are needed.

III. Opportunities:

1. **Cloud Computing Adoption:** Transitioning to cloud-based infrastructure can enhance scalability, reliability, and cost-effectiveness. Cloud solutions can address some infrastructure weaknesses.
2. **Mobile and IoT Integration:** Expanding web services to encompass mobile and IoT devices can broaden reach and engagement. This aligns with modern trends in higher education.
3. **Open-Source Frameworks:** Leveraging open-source tools and technologies can simplify development processes and reduce costs. This allows for more efficient and cost-effective development.
4. **Enhanced User Experience (UX):** Investing in UX design and user research can significantly improve user satisfaction and engagement. UX improvements directly translate into user satisfaction and better university image.
5. **Data-Driven Decision Making:** Utilizing analytics and data visualization tools can provide insights for optimizing web services and meeting user needs. Data analysis ensures the improvements are aligned with actual user requirements.
6. **Collaboration with COMSIT Units:** Synergistic collaborations with other COMSIT units can enhance operational efficiency and facilitate integration with university systems. Collaboration ensures smooth integration of web services into the university ecosystem.

IV. Threats:

1. **Evolving Cyber Threats:** The increasing sophistication of cyber threats poses a significant risk to the security and integrity of the university's web services. This requires proactive security measures.

2. **Emerging Technologies:** Rapid technological advancements necessitate continuous adaptation and upgrades to maintain competitiveness. Staying ahead of the technological curve is vital.
3. **Regulatory Compliance:** Stricter data privacy and security regulations can increase compliance costs and operational complexities. Staying up-to-date with regulations and meeting compliance is vital.
4. **Competition:** Other universities may have superior online presences, negatively impacting the University of Ilorin's global ranking. This necessitates a competitive advantage through continual improvement.
5. **Budget Constraints:** Limited funding may restrict the implementation of necessary upgrades and enhancements. Prioritization and efficient resource allocation are key to overcoming this challenge.

G. KEY PERFORMANCE INDICATORS (KPIs)

I. Website Performance & Availability:

1. **Uptime:** Percentage of time the website is operational and accessible (target: 99.99%). This is a fundamental measure of website reliability. Benchmark against leading universities' uptime.
2. **Page Load Speed:** Average time to load a page (target: under 2 seconds). This KPI directly impacts user experience. Benchmark against competitor universities and industry averages for higher education websites.
3. **Time to First Byte (TTFB):** Time taken from user request to receiving the first byte of data (target: under 200 milliseconds). This reflects server response speed. Benchmark against industry best practices for fast-loading websites.
4. **Website Traffic:** Total number of monthly visits (target: Specific, measurable target based on current traffic and growth projections). This indicates website reach and engagement. Benchmark against similar-sized universities and growth trends in higher education.
5. **Bounce Rate:** Percentage of visitors who leave after viewing only one page (target: below 40%). This KPI assesses user engagement. Benchmark against best practices for higher education websites.
6. **Average Session Duration:** Average time spent per visit (target: increase year-over-year). A longer session shows higher user engagement. Benchmark against competitor university websites.

II. User Experience (UX) & Engagement:

1. **User Satisfaction Score (e.g., Net Promoter Score - NPS):** Measures user loyalty and satisfaction (target: score of 70 or above). This is a crucial measure of overall user

experience. Benchmark against industry standards for user satisfaction in higher education.

2. **Conversion Rate:** Percentage of visitors completing a desired action (e.g., form submission, event registration) (target: Specific, measurable target based on desired actions). This KPI assesses the effectiveness of website calls to action. Benchmark against competitor universities' conversion rates on similar activities.
3. **Mobile Compatibility:** Percentage of mobile traffic with a positive user experience (target: 95% or higher). This ensures accessibility across devices. Benchmark against industry standards for mobile responsiveness.
4. **Accessibility Compliance:** Adherence to WCAG (Web Content Accessibility Guidelines) standards (target: AA or AAA compliance). This guarantees accessibility for users with disabilities. Benchmark against leading universities' accessibility scores.

III. Security & Reliability:

1. **Security Incidents:** Number of security breaches or vulnerabilities identified and addressed (target: zero). This ensures the website's security and integrity. Benchmark against leading universities' reported security incidents.
2. **Error Rate:** Percentage of failed requests (target: below 1%). This KPI indicates system stability and reliability. Benchmark against industry best practices for website error rates.
3. **Bug Resolution Time:** Average time taken to resolve reported bugs (target: within 24 hours for critical issues). This measure assesses responsiveness to technical issues. Benchmark against industry average for bug resolution time.
4. **Downtime Costs:** Financial impact of website downtime (target: minimize). This highlights the importance of uptime and the associated costs of downtime. Benchmark against the industry average cost of downtime for comparable websites.

IV. Content & SEO:

1. **Content Freshness:** Percentage of website content updated within a specified timeframe (e.g., 6 months) (target: 80% or higher). This KPI highlights the quality and timeliness of content. Benchmark against competitor universities' website content update frequency.
2. **Search Engine Ranking (SERP):** University's ranking on search engines for relevant keywords (target: improvement year over year). This measure assesses the website's visibility. Benchmark against competitor universities' rankings on major search engines.
3. **Social Media Engagement:** Number of followers, likes, shares, and comments on the university's social media pages (target: specific, measurable growth). This indicates engagement on social media platforms. Benchmark against competitor universities' levels of social media engagement.

V. Collaboration & Efficiency:

1. **Cross-Unit Collaboration:** Number of successful collaborations with other COMSIT units (target: increase year-over-year). This demonstrates effective integration within COMSIT.
2. **Project Completion Rate:** Percentage of web development projects completed on time and within budget (target: 90% or higher). This measure assesses project management effectiveness.
3. **Staff Training & Development:** Number of staff members trained on new technologies or skills (target: Specific, measurable target based on training needs). This shows a commitment to ongoing professional development.

H. STANDARD OPERATING PROCEDURE (SOP)

This SOP outlines the operational framework, responsibilities, and reporting structure for the Web Services Unit within the Computer Services and Information Technology (COMSIT) Directorate at the University of Ilorin. It aims to ensure efficient, consistent, and high-quality web services aligned with global best practices for world-class universities**.**

I.LINE OF COMMAND

Structure of Operations:

The Web Services Unit operates under the COMSIT Directorate and is structured into the following teams:

1. **Leadership & Coordination:** Unit Head
2. **Web Development & Engineering:** Lead Web Developer, Senior Web Developers, Junior Web Developers
3. **User Experience (UX) & Design:** UX Designer, UI/UX Designers
4. **Quality Assurance & Testing:** Quality Assurance Engineer
5. **Data Analytics & Performance:** Data Analyst
6. **Cybersecurity & Operations:** Web Security Specialist, Web System Administrator
7. **Project Management:** Project Manager
8. **Training & Support:** Training Coordinator

III. Responsibilities:

1. **Unit Head:** Strategic planning, resource allocation, budget management, performance monitoring, staff supervision, and overall unit performance.
2. **Web Development Team:** Designing, developing, implementing, and maintaining website functionality and applications.
3. **UX/UI Team:** Designing user-friendly interfaces and ensuring a positive user experience.
4. **Quality Assurance Team:** Ensuring website quality, stability, security and accessibility through rigorous testing.

5. **Data Analytics Team:** Monitoring website performance, user behavior, and identifying areas for improvement.
6. **Cybersecurity Team:** Implementing and maintaining security protocols to protect against cyber threats.
7. **Operations Team:** Managing website infrastructure and ensuring uptime and availability.
8. **Project Management Team:** Overseeing web development projects, ensuring timely delivery and adherence to budgets.

V. ESCALATION PROCEDURES:

1. **Technical Issues:** Escalate to the Lead Web Developer or Web Operations Engineer for technical support or infrastructure problems. Critical issues should be escalated immediately to the Unit Head.
2. **User Issues:** Escalate unresolved user issues to the Training Coordinator for guidance or to the Unit Head if a broader system issue is suspected.
3. **Security Incidents:** Immediately escalate all security incidents to the Web Security Specialist and the Unit Head.
4. **Project Management Issues:** Project-related escalations are handled by the Project Manager, and critical issues are escalated to the Unit Head.

VI. Reporting Lines:

1. All team leads report to the Unit Head.
2. The Unit Head reports to the appropriate COMSIT Director.

VIII. Review and Updates:

This detailed SOP provides a clear and structured framework for the operations of the University of Ilorin's Web Services Unit. By adhering to this SOP, the unit can ensure the delivery of high-quality, secure, and user-friendly web services that align with global standards for world-class universities.

This document outlines procedures for controlling, approving, accessing, storing, and retrieving documents within the University of Ilorin Web Services Unit. These procedures are designed to ensure document integrity, security, and efficient management.

J. CONTROL DOCUMENT

The following document types will be managed under this system:

Technical Documents: Design specifications, code documentation, testing plans, security protocols, and system architecture diagrams.

Operational Documents: Standard Operating Procedures (SOPs), incident reports, maintenance logs, and training materials.
Policy Documents: Web Services Unit policies, security policies, and data governance guidelines.
Project Documents: Project plans, timelines, budgets, and communication logs for all ongoing web development projects.
Legal Documents: Contracts, licenses, and other legal agreements related to web services.

II. Document Approval Process:
All documents will undergo a formal approval process based on their classification and sensitivity:

1. **Draft Documents:** Created and reviewed by the responsible individual or team.
2. **Review & Approval:** Documents are circulated for review by relevant stakeholders (e.g., team leads, Unit Head). Signatures or digital approvals will be obtained.
3. **Final Approval:** The Unit Head provides final approval for all documents, except those needing higher-level approval (e.g., policy changes). Higher-level approvals are routed through the appropriate channels within COMSIT and the university.
4. **Version Control:** All documents will have version numbers and revision dates. Changes will be documented in a revision log.

III. Access Control:
Access to documents will be controlled through a combination of methods:

1. **Role-Based Access:** Access is granted based on job responsibilities and security clearances. Users will only have access to documents relevant to their roles.
2. **Document Classification:** Documents are classified by sensitivity level (e.g., confidential, restricted, public). Access levels are determined accordingly.
3. **Secure Document Repository:** All documents are stored in a secure, password-protected document management system (DMS).
4. **Password Management:** Strong passwords are required, and regular password changes are enforced.
5. **Audit Trails:** The DMS will maintain audit trails to track document access, modifications, and deletions.
6. **User Training:** All personnel will undergo training on proper document handling and security protocols.

IV. Document Storage and Retrieval:

1. **Document Management System (DMS):** The Web Services Unit will use a designated DMS to store and manage all documents electronically. This system will provide version control, access control, and audit trails.

2. **File Naming Convention:** A standardized file naming convention will be used to ensure consistent organization.
3. **Document Metadata:** Appropriate metadata (e.g., document type, author, creation date, keywords) will be assigned to each document to facilitate searching and retrieval.
4. **Regular Backups:** Regular backups of the DMS are performed to prevent data loss. A robust disaster recovery plan is in place.
5. **Physical Documents:** If physical documents are necessary, they must be stored in a secure, controlled location with limited access.

K. FUTURE EXPANSION

This plan outlines potential areas for expansion and growth of the Web Services Unit, building on its current capabilities and aligning with the evolving needs of the University of Ilorin and advancements in web technologies.

I. Enhancements to Current Capabilities:

1. **Advanced Analytics & Reporting:** Invest in more sophisticated analytics tools and expertise to gain deeper insights into user behavior, website performance, and the effectiveness of digital marketing campaigns. This will allow for more data-driven decision-making and strategic planning.
2. **Improved Cybersecurity Posture:** Expand cybersecurity expertise and resources to proactively address evolving threats and ensure the ongoing security and integrity of the university's web infrastructure. This is crucial in the face of increasing cyber threats.
3. **Enhanced User Experience (UX) Design:** Further invest in UX/UI design capabilities, conducting regular user research to improve website usability, accessibility, and overall user satisfaction. Prioritizing user experience translates into improved website usage and reputation.
4. **Mobile-First Approach:** Develop a more mobile-first approach to web design and development, ensuring that the university's websites are fully optimized for mobile devices and provide an excellent user experience on any platform. This is critical in the mobile-first digital world.
5. **Content Management System (CMS) Upgrade:** Implement a more robust and scalable CMS that can support greater content creation, management, and publishing workflow efficiencies. This allows for improved efficiency and more streamlined content management.
6. **Artificial Intelligence (AI) Integration:** Explore the integration of AI-powered tools and technologies to automate tasks, personalize user experiences, and improve content creation and optimization. This is key to leveraging the latest technological advancements.

II. EXPANSION INTO NEW AREAS:

1. **Web Application Development:** Expand into the development of custom web applications that meet specific needs of different university departments or stakeholders. This will offer broader and more specialized services.
2. **Digital Marketing & SEO:** Develop in-house digital marketing expertise to increase website visibility and attract new audiences. This allows for proactive marketing initiatives.
3. **Virtual Reality (VR) and Augmented Reality (AR) Integration:** Explore the use of VR/AR technologies to enhance the online learning experience and provide immersive digital content. This is key to keeping the university at the cutting-edge of technology.
4. **Learning Management System (LMS) Integration:** Enhance integration with the university's LMS to provide a seamless online learning experience for students. This integrates the Web Services Unit more closely into the education process.
5. **Data Visualization and Reporting Dashboard:** Develop a sophisticated dashboard for visualizing key performance indicators (KPIs), website analytics, and other relevant data, providing real-time insights into the effectiveness of web services. This allows for improved efficiency in identifying areas for improvement.
6. **Digital Accessibility Services:** Expand services to address the growing need for web accessibility, ensuring that the university's online resources are accessible to users with disabilities. This fulfills a growing need for greater inclusion and inclusivity.

III. Strategic Partnerships and Collaboration:

1. **External Partnerships:** Establish partnerships with external vendors and technology providers to access advanced technologies and expertise. This allows for leveraging of external expertise and resources.
2. **Inter-Departmental Collaboration:** Foster greater collaboration with other departments and units across the university to ensure alignment of web services with the university's overall strategic goals. This integration ensures the university's web services are closely aligned with the broader university strategic goals.

IV. Resource Allocation:

Successful implementation of this expansion plan requires adequate investment in:

1. **Personnel:** Recruiting and training skilled personnel in areas such as data analytics, UX/UI design, cybersecurity, and AI.
2. **Technology:** Investing in new software, hardware, and infrastructure to support expanded services.
3. **Training & Development:** Providing ongoing professional development opportunities for staff to stay current with emerging technologies and best practices.

This expansion plan is designed to be iterative and adaptable. Regular reviews and adjustments will be necessary to reflect changes in technology, the needs of the university, and budgetary considerations. By proactively planning for future expansion, the Web Services Unit can ensure its continued success in supporting the University of Ilorin's digital transformation goals.

INTERFACING AREAS WITH OTHER COMSIT UNITS AND THE UNIVERSITY COMMUNITY

The Web Services Unit actively seeks synergies with other COMSIT units to ensure efficient and effective use of resources, improve services, and align with the overall goals of the University. This includes joint planning, shared resources, and collaborative training.This document outlines a framework for positive interactions and collaboration between the Web Services Unit and both internal (COMSIT) and external (university community) stakeholders. Regular review and adaptation are crucial to ensure that these processes remain aligned with the evolving needs of the University of Ilorin.

I. INTERFACING WITH COMSIT UNITS:

The Web Services Unit collaborates closely with several COMSIT units to ensure efficient and effective operations:

1. **Administration & Operations:** The Web Services Unit works with Administration & Operations for budget allocation, resource management, and strategic planning. This collaboration ensures alignment of resources with overall university goals.
2. **Network Operations Center (NOC):** The NOC provides crucial infrastructure support, ensuring robust internet connectivity and server management for optimal web service performance. Close coordination is essential for maintaining website uptime and security.
3. **Software & Hardware Installations, Repairs & Maintenance:** This unit provides technical support for server maintenance, upgrades, and troubleshooting. Collaboration ensures that the Web Services Unit's technical infrastructure functions efficiently.
4. **Software Development:** The Web Services Unit collaborates on coding standards, development methodologies (Agile), and the sharing of resources for creating custom applications or features. This ensures consistency and efficient use of resources.
5. **Cybersecurity & Multimedia:** The Cybersecurity team is crucial for implementing security protocols and protecting web services from cyber threats. The Multimedia team assists in creating engaging and visually appealing web content.
6. **Email Services & Helpdesk :** Collaboration ensures seamless integration of email functionalities into web services and provides a channel for addressing user inquiries related to the website.
7. **Training Unit:** The Web Services Unit works with the Training Unit to develop training programs for staff and users, ensuring that everyone is up-to-date on web services functionalities.

8. **IT Ideation & Innovation & Research & Development (TR&D):** The Web Services Unit collaborates with these units to explore new technologies and methodologies that enhance web service delivery and align with broader innovation goals.

II. Interfacing with the University Community:
The Web Services Unit serves the entire university community through a variety of interactions:

1. **Students:** The website provides crucial information for students, including academic resources, news, events, and support services. User feedback from students is actively sought and used to improve the website experience.
2. **Faculty & Staff:** The website provides resources for faculty and staff, including departmental information, research tools, and administrative services. Faculty and staff input is essential in maintaining current and accurate information.
3. **Alumni & External Stakeholders:** The website serves as a gateway for alumni engagement, promoting the university's reputation and building relationships with external stakeholders. Regular communication and updates are needed to maintain their engagement.
4. **General Public:** The website acts as a public-facing platform, providing information about the University to prospective students, researchers, and the general public. The website needs to be accessible and informative for this audience.

III. Communication and Feedback Mechanisms:
Effective communication is key to successful interfacing. The Web Services Unit will use the following mechanisms:

1. **Regular Meetings:** Scheduled meetings with relevant COMSIT units and university stakeholders.
2. **Project Management Tools (Trello, Asana):** For efficient communication and task management.
3. **Feedback Mechanisms:** Surveys, feedback forms, and other channels for collecting user feedback to improve web services.
4. **Internal Communications:** Regular newsletters and memos to keep stakeholders informed of updates and improvements.
5. **Service Level Agreements (SLAs):** Formal agreements with other COMSIT units outlining responsibilities and service expectations**.**

Conclusion:
The implementation of this blueprint positions the Web Services Unit to significantly enhance the University of Ilorin's web services. By adhering to the outlined procedures and strategies, the unit will achieve clear standards that improve web ranking, visibility, and user satisfaction. The robust framework for tracking KPIs allows for continuous optimization of digital strategies,

driving sustainable growth in web services. Through collaboration with other COMSIT units and a commitment to best practices in web development, the Web Services Unit will create a dynamic online environment that meets user needs while aligning with global standards in higher education. This proactive approach not only enhances the university's reputation but also contributes to its mission of providing quality education through innovative digital solutions. Regular review and adaptation of this blueprint are crucial to ensure ongoing relevance and effectiveness in meeting the evolving needs of the university and its stakeholders.

Prepared by:
Professor Rasheed Gbenga Jimoh, FNCS
Dr. Rasheed Adekola Tomori
Mr. Bolakale Abdulkadir Saka
Mr. Bolakale Aliyu Yusuff
Mrs. Florence Omodunke Fatoki
Mrs. Sarah Oluwafunmilayo Alabi
Mrs. Medinah Tanwa Salman
Engr Hussein Olanrewaju Akande
Mr. Yekeen Suleiman
Dr. Mrs. Aderinola Ololade Dunmade
Mrs. Medinat Omowumi Ayodeji
and Maintenance Unit
Mr. Tunde Olanrewaju
Mrs. Shakirat Adeboyin Oyeleke

Conclusion

This Operational Blueprint sets out the mandate, structure, and strategic direction of each of the twelve units within the Directorate of Computer Services and Information Technology (COMSIT) for the 2025–2035 period. Taken together, the unit-level blueprints presented above constitute the Directorate's roadmap for delivering reliable, secure, and innovative ICT services in support of the University of Ilorin's academic, research, and administrative mission. Implementation will be reviewed periodically to ensure continued alignment with the University's strategic goals and the evolving digital landscape.

Appendices

Supporting documents, detailed organograms, policy references, and other supplementary material for this blueprint will be attached here.