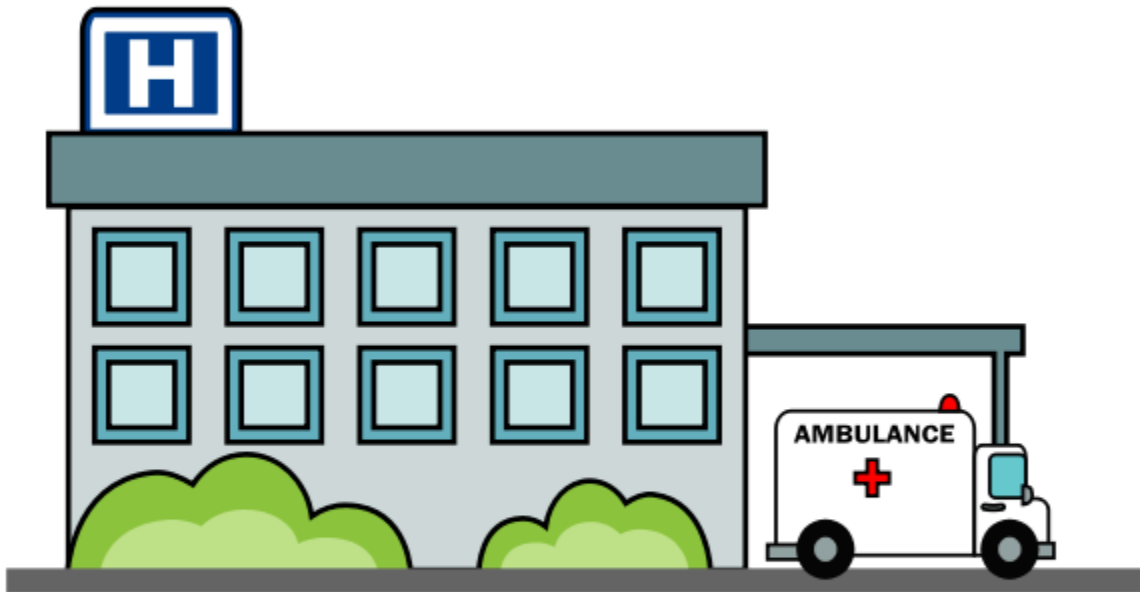# NGOMA DZA VHATEI EXPERT CHANGE RECOMMENDATION UTHUKELA DISTRICT MUNICIPALITY HOSPITAL

GROUP MEMBERS
Mukhola Thuso
Muguvhana Mbambala
Maphaha Livhuwani
Mohlala Surprise

TABLE OF CONTENTS

1. Upgrade and Standardize Hardware

- **Recommendation**: Replace outdated computers and printers with newer, more efficient models to reduce downtime and improve overall system reliability.
- **Justification**: Outdated hardware leads to frequent breakdowns and maintenance costs, which disrupt critical hospital functions. Upgrading and standardizing hardware across departments will enhance operational continuity.
- **Implementation**: Use cost-effective models that are compatible with the hospital's needs, and ensure there is a unified maintenance contract for all hardware to streamline support.

2. Implement a Secure Network Infrastructure

- **Recommendation**: Establish a secure and segmented network infrastructure with firewalls, encrypted Wi-Fi access points, and VLANs (Virtual Local Area Networks) for different departments.
- **Justification**: Segmentation enhances data security, reduces the risk of unauthorized access, and limits the impact of potential cyber threats on sensitive patient data.
- **Implementation**: Install firewalls and routers configured with network segmentation to separate administrative, medical, and guest network traffic. Use WPA3 encryption for wireless networks to secure hospital-wide connectivity.

3. Centralized Data Storage with Backup Solutions

- **Recommendation**: Implement a centralized data storage solution with automated backup and recovery capabilities.
- **Justification**: Currently, missing patient files are a major issue. Centralized storage will improve data accessibility, integrity, and reduce the risk of data loss.
- **Implementation**: Set up a Network Attached Storage (NAS) or cloud-based system for central storage, with regular automated backups. Include a disaster recovery plan and train ICT staff on data retrieval processes.

4. Enhance Security Protocols and Access Control

- **Recommendation**: Establish role-based access controls (RBAC) and strengthen authentication protocols to protect sensitive data.
- **Justification**: Role-based access prevents unauthorized access to critical systems and ensures that users only access data relevant to their role, enhancing data security.
- **Implementation**: Configure the system to require multi-factor authentication for administrative access and audit user activity regularly. Install software for real-time monitoring of network traffic to detect potential breaches early.

5. Deploy New Software Solutions for Hospital Management

- **Recommendation**: Implement or upgrade to integrated hospital management software (e.g., Electronic Health Records (EHR) and Enterprise Resource Planning (ERP) systems) to streamline operations.

- **Justification**: An integrated system allows for better tracking of patient records, billing, inventory, and supply chain management, significantly improving hospital service efficiency.
- **Implementation**: Work with vendors to customize software for the hospital's needs and train staff on using these systems effectively.

6. Comprehensive Staff Training Program

- **Recommendation**: Conduct comprehensive training for ICT staff on network management and hospital staff on the new systems.
- **Justification**: Properly trained staff can troubleshoot minor issues independently, which reduces the reliance on IT support and ensures minimal disruptions.
- **Implementation**: Develop a phased training plan. Begin with ICT staff training on system installation, troubleshooting, and security protocols. Follow with training sessions for medical and administrative staff on how to use new software effectively.

7. Establish Ongoing Maintenance and Support Contracts

- **Recommendation**: Set up maintenance and support contracts with vendors to ensure hardware and software systems receive regular updates and repairs.
- **Justification**: Preventive maintenance minimizes downtime and extends the life of hardware and software assets, which is essential for a critical healthcare environment.
- **Implementation**: Negotiate contracts with vendors for regular maintenance check-ups, including hardware diagnostics, software updates, and 24/7 technical support.

8. Regular System Testing and Monitoring

- **Recommendation**: Implement a structured testing schedule to regularly assess the performance and security of IT systems.
- **Justification**: Regular testing helps detect vulnerabilities early and ensures that the network and applications remain reliable and secure.
- **Implementation**: Conduct quarterly network testing and annual security audits. Use automated monitoring tools to provide alerts for system anomalies or unauthorized access attempts.

9. Optimize Network Bandwidth and Connectivity

- **Recommendation**: Upgrade the network's bandwidth capacity and configure it to prioritize critical hospital services.
- **Justification**: Reliable connectivity is crucial for daily operations and communications between departments and external providers.
- **Implementation**: Evaluate current bandwidth usage and upgrade as necessary. Implement Quality of Service (QoS) policies to prioritize high-priority services, such as EHR access and inter-department communications.

10. Set Up a Feedback and Continuous Improvement Loop

- **Recommendation**: Establish a system for hospital staff to provide feedback on the new IT systems and identify areas for further improvement.

- **Justification**: Ongoing feedback ensures the system continues to meet user needs and can adapt to changing requirements in hospital operations.
- **Implementation**: Create a feedback platform where staff can report issues or suggestions, and assign an IT team member to review feedback and prioritize adjustments.

REFERENCES

Laudon, K.C. & Laudon, J.P., 2020. *Management Information Systems: Managing the Digital Firm*. 16th ed. Harlow: Pearson.

Project Management Institute, 2021. *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*. 7th ed. Newtown Square, PA: Project Management Institute.

Stallings, W., 2019. *Foundations of Security: What Every Programmer Needs to Know*. 2nd ed. New York: Pearson.