HospitalGuard: Network Security Policy and Risk Assessment for OOUTH

Network Security Policy & Risk Management Report

Institution: Olabisi Onabanjo University Teaching Hospital (oouth.com), Sagamu, Ogun State
Domain: Healthcare Cybersecurity

1. Risk Assessment

Organization Type: Tertiary Teaching Hospital

Critical Digital Assets Identified:

- ✓ Electronic Medical Records (EMR)
- ✓ Laboratory Information Systems (LIS)
- ✓ Radiology Information Systems (RIS)
- ✓ Staff and Patient Personal Data
- ✓ Networked Medical Devices (e.g., ECG monitors)
- ✓ Internal Wi-Fi Infrastructure
- ✓ Communication Platforms (Email, Messaging)
- ✓ Power Supply Infrastructure and Backup Generators

Threats & Vulnerabilities

Asset	Threat	Risk Rating
EMR Systems	Ransomware Attacks	High
Laboratory Information Systems	Unauthorized Access	High
Radiology Information Systems	Outdated Software & Systems	Medium
Staff and Patient Data	Phishing & Social Engineering	High
Medical Devices	Lack of Security Configurations	Medium
Hospital Networks	DDoS (Denial-of-Service) Attacks	High
Power Infrastructure	Fuel Theft & Physical Intrusion	High
Patient Monitoring Devices (e.g. ECG)	Malware Embedded in Firmware	Medium

---

2. Network Security Policy

Purpose & Scope:
To safeguard OOUTH's digital infrastructure, ensuring confidentiality, integrity, and availability of sensitive healthcare data.

User Responsibilities:

- ✓ Use strong passwords and change them periodically.
- ✓ Report suspicious activity or incidents immediately.
- ✓ Access data strictly within one's role.
- ✓ Do not share login credentials under any circumstances.

Access Control Policy:

- ✓ Apply Role-Based Access Control (RBAC).
- ✓ Enable Multi-Factor Authentication (MFA) for sensitive systems.
- ✓ Regularly audit and update access privileges.

Data Protection Policy:

- ✧ Encrypt all data in transit and at rest.
- ✧ Implement regular, automated, and offsite backups.
- ✧ Monitor data flow with DLP (Data Loss Prevention) systems.

Incident Response Plan:

- ✓ Establish a trained Incident Response Team (IRT).
- ✓ Document clear procedures for identifying and containing threats.
- ✓ Communicate incidents promptly to management and affected departments.
- ✓ Conduct a post-incident review to improve future responses.

Training & Awareness:

- ➢ Host regular staff cybersecurity workshops.
- ➢ Circulate educational material (flyers, internal email tips).
- ➢ Run phishing simulations to improve staff awareness.

3. Presentation Feedback Summary

Strengths:

- ✓ Clear and structured identification of threats and risks.
- ✓ Well-defined roles, responsibilities, and policies.

Suggestions for Improvement:

- ✓ Expand device-specific protocols, especially for smart medical devices.
- ✓ Include provisions for vendor systems and third-party access controls.

4. Final Reflection

As technology becomes more integrated into healthcare, institutions like OOUTH must prioritize digital security. Continuous monitoring, staff education, infrastructure investment, and policy updates are essential to defend against ever-evolving cyber threats.