UITH Cybersecurity Policy Project
University of Ilorin Teaching Hospital (UITH)
Cybersecurity Policies and Procedures to Address Audit Vulnerabilities
Prepared by: ALUBARIKA ABDULAZEEZ
Date: July 16, 2025
Submitted to: Kuagi Resources, UITH, MRS BLESSING ABBEY

TABLE OF CONTENT

1.0 SUMMARY

The University of Ilorin Teaching Hospital (UITH), a Nigerian federal healthcare institution, has faced significant data breaches over the past five years, resulting in financial and reputational damage. A recent security audit identified 15 critical vulnerabilities, prompting the development of this cybersecurity policy project. This document outlines a targeted Access Control Policy, a supporting procedure for managing privileged accounts, and a dissemination plan to ensure employee awareness and compliance. By addressing the most severe vulnerabilities, UITH aims to enhance data security, protect patient information, and align with regulatory standards such as the Nigeria Data Protection Regulation (NDPR).

2.0 OVERVIEW

UITH operates over 10 medical facilities, including departments for Obstetrics & Gynecology, ENT, Surgery, and General Outpatient Services. Over the past five years, data breaches have compromised sensitive patient and organizational data, necessitating urgent action. A new Chief Information Security Officer (CISO) commissioned a comprehensive security audit, revealing vulnerabilities such as unauthorized access, weak passwords, and unencrypted data. This project addresses these issues through policy development, focusing on access control to mitigate the most critical risks.

3.0 TOP 5 VULNERABILITIES AND RANKINGS

A security audit identified 15 vulnerabilities, prioritized based on their impact on confidentiality, integrity, and availability, as well as their likelihood of exploitation in a healthcare context. The top five vulnerabilities, recommended policies, and justifications are presented below.

. RANK	VULNERABILITY	. POLICY	JUSTIFICATION
1.	Unauthorized escalated privileges	Access Control Policy	Allows attackers to bypass controls and access sensitive patient data, posing a critical risk.
2.	Unencrypted sensitive files	Data Encryption Policy	Risks exposure of Protected Health Information (PHI), violating confidentiality and regulations
3.	Weak passwords (40% cracked in 6 hours)	Password Protection Policy	Weak passwords are a primary attack vector, enabling unauthorized access.
4.	Unpatched servers	Server Security Policy	Unpatched systems are vulnerable to known exploits, risking ransomware attacks.

5.	Permissive firewall rules	Network Security Policy	Allows unauthorized traffic, undermining network security.

These priorities were informed by research from the Top Computer Security Vulnerabilities resource (https://www.n-ale.com/features/computer-security-vulnerabilities) and healthcare cybersecurity best practices.

4.0. UITH ACESS CONTROL POLICY

Version 1.0 | Effective Date: July 15, 2025

1. OVERVIEW
Access control ensures that only authorized individuals access UITH's systems, networks, and data, protecting patient and organizational information.

2. PURPOSE
To establish standards for granting, managing, and revoking access, preventing unauthorized access and ensuring compliance with regulatory requirements.

3. SCOPE
Applies to all UITH employees, contractors, and third parties accessing UITH systems, including servers, databases, and applications.

4. POLICY
4.1. Principle of Least Privilege: Users receive only the access necessary for their job functions.
4.2. Account Management:
- Accounts for terminated employees must be disabled within 24 hours.
- Privileged accounts require approval from the IT Security Manager.
4.3. Access Reviews: Conduct quarterly audits to verify access rights.
4.4. Multi-Factor Authentication (MFA): Required for all privileged accounts and remote access.
4.5. Unauthorized Access: Attempts to access systems without Ascending-Ordered List without authorization are prohibited.

5. Compliance
Non-compliance may result in disciplinary action, including termination and legal consequences. The IT Security Team will audit compliance annually.

6. Definitions
- Privileged Account: An account with elevated access rights.
- MFA: Authentication requiring two or more verification factors.

Contact: IT Security Manager, security@uith.gov.ng

5.0 PROCEDURE : Managing Privileged Accounts

Version 1.0 | Effective Date: July 15, 2025

Purpose: To ensure secure management of privileged accounts per the UITH Access Control Policy.

Scope: Applies to IT administrators and the IT Security Team.

Steps:
1. Request Creation:
   - Submit a Privileged Account Request Form to the IT Security Manager, specifying job role and access needs.
   - Form available at intranet.uith.gov.ng/security.
2. Approval:
   - IT Security Manager reviews and approves/denies within 48 hours.
   - Approved requests are logged in the Access Control Database.
3. Account Setup:
   - IT Admin creates the account with least privilege settings.
   - Enable MFA using UITH's authenticator app (e.g., Microsoft Authenticator).
4. Monitoring:
   - Use SIEM tools to log privileged account activity.
   - Review logs weekly for unauthorized access attempts.
5. Review and Revocation:
   - Conduct quarterly access audits using the Access Control Database.
   - Disable accounts for terminated employees within 24 hours via Active Directory.
6. Documentation:
   - Maintain records of approvals, audits, and revocations for 3 years.

Tools Required:
- Active Directory for account management.
- SIEM solution (e.g., Splunk) for logging.
- MFA app for authentication.

Contact: IT Security Team, security@uith.gov.ng

6.0 UITH INFORMATION SECURITY POLICY IMPLEMENTATION AND DISSEMINATION PLAN

Version 1.0 | Effective Date: July 15, 2025

1. Objective
To ensure all UITH employees and contractors are aware of and comply with information security policies, protecting patient and organizational data.

2. Dissemination Tasks
- Publish policies on the UITH intranet (intranet.uith.gov.ng/security) by July 20, 2025.
- Email all employees a policy summary and link to full documents by July 22, 2025.
- Display policy posters in break rooms and IT areas by July 25, 20251.
- Require employees to acknowledge policy receipt via an online form within 7 days.

3. Training Program
- Conduct mandatory security awareness training by August 15, 2025:
  - Format: In-person (on-site staff) and virtual (remote staff).
  - Content: Policy overview, access control, encryption, and incident reporting.
  - Duration: 1 hour per session.
- Provide role-specific training for IT staff on privileged account management by August 20, 2025.
- Offer refresher training annually and for new hires within 30 days of onboarding.

4. Evaluation Methods
- Administer a policy knowledge quiz post-training (80% pass rate required).
- Conduct simulated phishing tests quarterly to assess employee awareness.
- Perform annual policy compliance audits by the IT Security Team, starting January 2026.
- Collect employee feedback via surveys by September 15, 2025, to identify gaps.

5. Departments Involved
- HR: Coordinate training and policy acknowledgment.
- IT: Manage intranet, training platforms, and audits.
- Compliance: Ensure alignment with regulatory requirements.
- Department Heads: Enforce policy adherence within teams.

6. Timeline
- July 20–25, 2025: Policy dissemination.
- August 1–20, 2025: Training sessions.
- September 15, 2025: Feedback collection.
- January 2026: First compliance audit.

Contact: IT Security Manager, security@uith.gov.ng

7.0. CONCLUSION

The UITH Cybersecurity Policy Project addresses critical vulnerabilities identified in a recent security audit, with a focus on unauthorized escalated privileges. The Access Control Policy, supported by a detailed procedure for managing privileged accounts, establishes a robust framework for securing access to sensitive systems and data. The dissemination and evaluation plan ensures employee awareness and compliance, fostering a culture of cybersecurity. By implementing these measures, UITH can protect patient information, comply with regulations like the NDPR, and rebuild its reputation as a trusted healthcare provider.

8.0. Reference

- SANS Security Policy Project Templates: https://www.sans.org/security-resources/policies/
- Information Security Policy (video): https://youtu.be/Z1KqM1OpM8o
- Top Computer Security Vulnerabilities: https://www.n-ale.com/features/computer-security-vulnerabilities
- Information Security Policy - A Development Guide: https://www.sans.org/white-papers/1331/
- Technical Writing for IT Security Policies in Five Easy Steps: https://www.sans.org/white-papers/1492/