UNIVERSITY OF MINES AND TECHNOLOGY
TARKWA

FACULTY OF COMPUTING AND MATHEMATICAL SCIENCES
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DESIGN AND IMPLEMENTATION OF AN ORGANIZATIONAL INFORMATION SECURITY FRAMEWORK

BY
OWARE KELVIN

(INDEX NUMBER: FOE.41.008.127.22)

CE 3C

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR SECOND LAB PROJECT

IN INFORMATION AND CYBER SECURITY(CE372)

LECTURER: DR. ERIC AFFUM

TARKWA

JULY 2025

DECLARATION

Self-Declaration Statement on AI Usage and Academic Integrity

I, **OWARE KELVIN**, hereby declare that this project titled:

"Design and Implementation of an Organizational Information Security Framework"

is entirely my own original work.

I affirm that:

- I have **not used AI tools** (e.g., ChatGPT, Bard, or others) to generate full sections of this report.
- Any use of AI or digital tools was strictly limited to **grammar checks, formatting help, or idea prompts**, and did **not replace my personal understanding or effort**.
- I fully understand all the content presented in this project and can explain it independently if required.
- I have not copied, paraphrased, or submitted any material that I do not fully comprehend.

I understand that any **false declaration**, **plagiarism**, or **excessive reliance on AI tools** may result in **disqualification**, **failure**, or **disciplinary action**.

Student's Name: _____

Student ID: _____

Signature: _____

Date: _____

ABSTRACT

This project presents the design and implementation of a comprehensive Information Security Framework for a simulated mid-sized organization that recently suffered a phishing-related security incident. The breach exposed critical weaknesses in the organization's cybersecurity posture, including a lack of formal security policies, limited user awareness, and inadequate technical controls. The project adopts a structured approach beginning with a security audit and risk assessment to identify vulnerabilities and assess the organization's exposure to various threats. Legal and ethical considerations are analyzed with reference to relevant data protection laws such as the **Ghana Data Protection Act** and the **General Data Protection Regulation (GDPR)**. A detailed information security policy is developed, addressing key areas such as acceptable use, password management, access control, and incident response. Additionally, the project evaluates and recommends cost-effective security tools such as firewalls, antivirus software, encryption mechanisms, and multi-factor authentication. A user training and awareness plan is also proposed to cultivate a culture of cybersecurity within the organization. This work aims to simulate the responsibilities of a real-world information security professional and provides practical, legally compliant, and scalable solutions to strengthen organizational security and reduce the risk of future cyber incidents.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all those who supported me throughout the development of this project titled: **"Design and Implementation of an Organizational Information Security Framework."** First and foremost, I would like to thank **DR. ERIC AFFUM**, my course supervisor, for their guidance, feedback, and encouragement throughout the course of this project. Their insights into information security concepts were truly invaluable. I am also grateful to my **family and friends** for their constant support and motivation, especially during challenging moments of the project.

Table of Contents

CHAPTER 1

ORGANIZATIONAL CONTEXT AND PROBLEM DEFINITION

1.1 Introduction

Eastern Valley Hospital, a private healthcare provider in Ghana, recently experienced a phishing attack that compromised over 300 patient records. The breach exposed significant weaknesses in the hospital's information security practices, including poor password management, lack of user training, and absence of a centralized security policy. This report presents a practical, cost-effective, and legally compliant information security framework tailored to the hospital's size and needs. A comprehensive audit revealed that while basic IT systems were in place, critical safeguards such as encryption, multi-factor authentication, and access control were missing or misconfigured.

To address these issues, the project outlines a phased approach covering:

- A detailed security risk assessment
- A new security policy framework based on industry best practices
- Legal and ethical compliance aligned with Ghana's Data Protection Act
- Selection and deployment of affordable, open-source tools
- A user training and awareness program focused on phishing prevention and data handling
- A practical implementation roadmap with cost and timeline estimates

The proposed solution requires a modest budget of approximately **GHS 16,000** and can be implemented within 8 weeks. If adopted, this framework will help the hospital significantly reduce security risks, ensure legal compliance, and protect sensitive patient data with minimal operational disruption.

1.2 Organization Overview

Eastern Valley Hospital is a privately owned, mid-sized healthcare facility located in the Eastern Region of Ghana. The hospital provides outpatient care, diagnostics, and emergency services to a patient population exceeding 10,000 annually.

The organization employs approximately **250 staff members**, distributed across the following key departments:

- **Clinical Services** (Doctors, Nurses, Lab Technicians)

- **Records and Patient Management**
- **Administration and Finance**
- **IT and Systems Support**

In recent years, the hospital has begun transitioning to digital operations, including cloud-based electronic medical records (EMR), online appointment systems, and internal communication via Google Workspace.

1.3 Summary of the Security Incident

In **March 2024**, the hospital experienced a **phishing attack** targeting an administrative employee. The attacker posed as a member of the IT team and sent an email requesting login verification via a fake link. The staff member unknowingly entered their credentials, which were then used to access and download sensitive patient information.

The breach exposed the personal and medical data of over **300 patients**, triggering internal panic and a formal report to Ghana's Data Protection Commission. Though the damage was limited due to a timely response by the IT team, the event revealed deeper systemic weaknesses.

1.4 Identified Problems and Security Gaps

The security audit conducted after the incident revealed several critical issues:

- Lack of formal security policies and procedures
- Use of weak passwords and no multi-factor authentication
- Inadequate employee awareness of cyber threats
- Outdated antivirus software and no email filtering controls
- No incident response or breach reporting mechanism
- Absence of encryption for stored or backed-up patient data

These gaps present not only technical risks but also serious legal and ethical concerns, especially under Ghana's Data Protection Act.

1.5 Project Goals and Scope

This project aims to design and recommend a **comprehensive information security framework** tailored to the hospital's context. The key objectives are:

- Conduct a security audit and risk assessment
- Ensure legal and ethical compliance
- Develop a structured information security policy
- Recommend practical security tools and technologies

- Design a user awareness and training program
- Present a phased implementation roadmap

Scope limitations:

- Focus is placed on digital infrastructure and human behavior.
- Physical security (e.g., building access, CCTV) is out of scope.

1.6 Approach and Methodology

The following steps were taken to complete the project:

1. Interviews with IT and administrative staff to understand workflows and current practices
2. System observation to identify vulnerabilities and user behavior
3. Gap analysis comparing current practices with legal and industry standards (e.g., ISO 27001)
4. Tool evaluation based on cost, compatibility, and ease of use
5. Policy and training design using best practices and healthcare case studies

CHAPTER 2

SECURITY AUDIT AND RISK ASSESSMENT

2.1 Overview of Current Security Posture

At the time of the audit, Eastern Valley Hospital's IT security was found to be fragmented, informal, and reactive. While the hospital had adopted digital tools like Google Workspace and a cloud-based EMR system, there was no centralized security management or written information security policy.

Key weaknesses included:

- Basic antivirus software on some devices, but outdated on others
- No multi-factor authentication (MFA) for email or EMR access
- Shared accounts used by admin staff in the records department
- No structured approach to password management
- No awareness training on phishing or cybersecurity risks

The hospital lacked a dedicated IT security role, and most technical decisions were made by a general IT technician focused more on troubleshooting than prevention.

2.2 Threat Identification

The following threat categories were identified as most relevant:

Threat Category	Examples Affecting the Hospital
Social Engineering	Phishing emails, impersonation of staff
Malware & Ransomware	Infections via email attachments or USB drives
Insider Threats	Accidental disclosure, staff negligence
Credential Theft	Weak passwords, lack of MFA
System Misconfiguration	Insecure file sharing, open admin access

Phishing remains the **most immediate threat**, as proven by the recent breach.

2.3 Vulnerability Assessment

The vulnerabilities observed during the audit include:

- **Lack of MFA**: All users access EMR and email using only usernames and passwords.
- **Password reuse**: Staff use the same passwords across platforms, often written down.
- **No email filtering**: Spam and phishing emails are not automatically filtered.
- **USB exposure**: Any flash drive can be plugged into staff computers without restriction.
- **Plaintext data**: Some patient files are stored unencrypted on shared local drives.
- **No backup policy**: Backups are performed manually and irregularly.

These vulnerabilities increase the risk of data breaches, regulatory non-compliance, and operational downtime.

2.4 Risk Matrix and Analysis

Risk	Likelihood	Impact	Risk Level
Phishing attack on staff	High	High	**Critical**
Unauthorized access to EMR	High	High	**Critical**
Malware infection via USB/email	Medium	High	High
Data loss due to accidental deletion	Medium	Medium	Moderate
Unauthorized sharing of patient records	Medium	High	High
Power failure affecting data availability	Low	High	Moderate

These risk ratings indicate that human error and poor system access control are the most urgent priorities to address.

CHAPTER 3

LEGAL, REGULATORY, AND ETHICAL COMPLIANCE

3.1 Overview of Applicable Laws and Regulations

Ghana Data Protection Act, 2012 (Act 843)
This Act governs how personal data must be collected, processed, stored, and shared in Ghana. For a healthcare facility like Eastern Valley Hospital, compliance is mandatory and failure to adhere can lead to sanctions or lawsuits.

Key legal requirements include:

- **Data minimization** – Collect only what is necessary for care
- **Consent** – Patients must be informed about how their data is used
- **Security safeguards** – Systems must be in place to prevent unauthorized access, loss, or theft of data
- **Breach notification** – All breaches must be reported to the Ghana Data Protection Commission promptly
- **Data subject rights** – Patients have the right to access and correct their data

General Data Protection Regulation (GDPR)

Although GDPR is a European regulation, it influences best practices globally and applies if the hospital collaborates with international partners or handles EU patient data.

GDPR emphasizes:

- Lawful data processing
- Purpose limitation
- Data minimization
- Accuracy and transparency
- Strong data protection measures
- Strict breach reporting requirements

3.2 Current Compliance Status of Eastern Valley Hospital

An analysis of the hospital's current practices reveals several areas of non-compliance:

Legal Requirement	Current Status	Risk Level
Registration with DPC	Not registered	High
Data protection officer appointed	No dedicated officer	High
Privacy policy for patients	Not developed	High
Secure data storage (encryption)	Not implemented	High
Staff awareness of data regulations	Very low	High
Breach notification protocol	Not in place	High

These gaps not only risk legal consequences but also damage patient trust and organizational reputation.

3.3 Ethical Considerations

In addition to legal obligations, the hospital must uphold ethical responsibilities inherent to healthcare:

Patient Privacy and Confidentiality

Patients entrust healthcare workers with their most sensitive information. Improper handling, even if unintentional, can cause emotional harm and erode trust in the healthcare system.

Informed Consent and Transparency

Patients must be made aware of how their data is used. Collecting or sharing information without patient knowledge breaches ethical standards even if it doesn't violate a law directly.

Monitoring and Surveillance

While staff activity monitoring may be required for security, it must be balanced with respect for employee privacy. Transparency about such practices is essential.

Access Control Ethics

Role-based access must be enforced to ensure that only those with a legitimate need (e.g., a treating doctor) can access patient data. Ethical lapses occur when information is accessed out of curiosity or convenience.

3.4 Compliance Gap Analysis

Area	Required Practice	Current Practice	Gap Severity
Data Protection Officer	Appointed and trained	Not assigned	High
Privacy Policy	Available to patients in clear language	Not available	High
Staff Training	Mandatory for all employees handling patient data	Not conducted	High
Patient Data Access	Strictly controlled and monitored	Shared passwords, poor logging	High
Data Encryption	Required for all sensitive data	Not implemented	High
Breach Notification Procedure	Documented and rehearsed	No process in place	High

CHAPTER 4

SECURITY POLICY AND GOVERNANCE FRAMEWORK

4.1 Policy Development Strategy

Developing a security policy for Eastern Valley Hospital required a balance between industry best practices, regulatory requirements, and the realities of a mid-sized healthcare facility. The proposed policy framework draws from:

- ISO/IEC 27001 principles
- Ghana Data Protection Act, 2012
- Observations from the hospital's security audit
- Consultation with staff from the IT and Records departments

Policies are written to be **clear**, **enforceable**, and **scalable** as the hospital grows.

4.2 Acceptable Use Policy (AUP)

This policy sets guidelines for how employees may use the hospital's IT resources:

- All devices (computers, mobile phones, tablets) must be used for authorized hospital tasks only.
- Personal software and apps may not be installed on hospital devices.
- Staff must not access inappropriate websites or open unsolicited attachments/emails.
- All activity on hospital systems is subject to monitoring by IT for security purposes.
- Staff are responsible for locking their screens when stepping away from workstations.

4.3 Password and Authentication Policy

Passwords are a frontline defense and must be managed properly. This policy enforces:

- Passwords must be at least **12 characters** long and include numbers, letters, and symbols.
- Passwords must be changed every **90 days**.
- **Multi-Factor Authentication (MFA)** is mandatory for accessing EMR systems, email, and financial records.
- Default passwords (e.g., from vendors) must be changed immediately.
- Passwords must never be shared or written down in visible places.

4.4 Access Control Policy

To prevent unauthorized access and protect patient privacy, the hospital will implement **Role-Based Access Control (RBAC)**:

- Every employee is assigned access only to the systems and data required for their role.
- Shared accounts are strictly prohibited.
- Access logs will be reviewed quarterly to detect anomalies.
- Any change in employee role or termination must trigger an access review.

Access Control Roles Example:

Role	**Access Level**
Doctor	Full access to patient EMRs
Nurse	Partial access (treatment logs only)
Records Staff	Input and query permissions
Admin	No medical data access

4.5 Data Protection and Classification Policy

To ensure data is handled according to its sensitivity, the following classifications are introduced:

Data Type	**Classification**	**Handling Instructions**
Patient EMR	Confidential	Encrypt at rest and in transit
Financial Records	Restricted	Access limited to Finance team only
HR Documents	Confidential	Stored on secure drive, encrypted backups
Hospital Policies	Public	Accessible to all staff and posted internally

- Sensitive data may not be shared via personal email or messaging platforms.
- Data must be **backed up weekly**, with backups encrypted and stored off-site.

4.6 Incident Reporting and Response Policy

All staff play a role in keeping the hospital secure. This policy outlines the process to follow if an incident occurs:

- Any **phishing email**, **suspicious file**, or **unusual system behavior** must be reported to IT immediately.
- A standardized **incident report form** will be available via the hospital intranet.
- The IT department must respond within **1 hour** to critical incidents.
- All reported incidents will be logged and reviewed monthly to detect recurring issues.
- Serious breaches (e.g., patient data theft) must be reported to the Ghana Data Protection Commission within 72 hours.

4.7 Governance Structure and Roles

A clear governance model ensures that policies are not just written — but enforced.

- **Data Protection Officer (DPO)**: Ensures legal compliance and manages privacy issues
- **IT Security Lead**: Oversees implementation of technical controls
- **Department Heads**: Enforce policy adherence within their teams
- **All Staff**: Responsible for secure behavior and reporting incidents

A Policy Review Committee, consisting of representatives from IT, HR, and Administration, will meet biannually to update the framework.

CHAPTER 5

TECHNICAL CONTROLS AND TOOLS

5.1 Tool Selection Principles

In selecting tools for Eastern Valley Hospital, the goal was to strike a balance between **effectiveness, affordability, and ease of use**. The following criteria were used:

- **Cost-effectiveness**: Preference given to open-source or low-cost tools
- **Compatibility**: Must integrate with existing systems (Windows OS, cloud-based EMR, Google Workspace)
- **User-friendliness**: Minimal learning curve for IT staff and end users
- **Security coverage**: Must protect against top risks: phishing, malware, unauthorized access, and data theft

5.2 Network and Perimeter Security

pfSense (Firewall Solution)

- Open-source firewall/router that provides stateful packet inspection, VPN support, and traffic filtering
- Helps isolate hospital departments into separate VLANs (e.g., clinical vs admin)
- Includes Intrusion Detection/Prevention capabilities via Snort plugin

Why it's ideal: pfSense offers **enterprise-grade network control** at zero licensing cost. It supports scalability and secure remote access.

5.3 Endpoint Protection and Malware Defense

Bitdefender GravityZone Business Security

- Cloud-managed antivirus and anti-malware system
- Provides real-time protection, behavior monitoring, and centralized reporting
- Lightweight and suitable for medical-grade systems with minimal disruption

Why it's ideal: Bitdefender offers **high detection rates** and easy deployment across hospital devices at a **reasonable cost**.

Additional Measure:

- **Windows Group Policy settings** will be used to **block unauthorized USB devices**, reducing the chance of infections via flash drives.

5.4 Access Management and Authentication

Google 2-Step Verification (MFA)

- Already available through the hospital's Google Workspace subscription
- Easy to activate for staff email and shared documents

EMR Role-Based Access Control (RBAC)

- User roles (Doctor, Nurse, Admin) will be configured in the EMR system
- Permissions limited to what each role requires

Why it's ideal: Both solutions use existing infrastructure, meaning **zero extra cost** and **minimal setup time**.

5.5 Data Protection and Encryption

VeraCrypt (Full-Disk Encryption)

- Free and open-source disk encryption software
- Encrypts laptops, USB drives, and backup volumes
- Adds a strong layer of protection for portable devices or lost/stolen hardware

Encrypted Cloud Backups

- Weekly encrypted backups will be stored offsite using a secure cloud provider
- Google Drive's built-in encryption and optional third-party backup tools (e.g., IDrive) will be used

5.6 Monitoring and Incident Detection

While a full Security Information and Event Management (SIEM) system may be beyond current budget, the following lightweight options are recommended:

- **Windows Event Logs + Centralized Log Collection** using built-in tools or open-source syslog solutions
- Regular **manual log review** by the IT lead until automation is feasible
- **Email phishing simulation tools** like **GoPhish** will be used quarterly to test staff awareness

CHAPTER 6

HUMAN FACTORS AND AWARENESS PROGRAM

6.1 Why Human Behavior Matters

Even with strong technical controls, human error remains the biggest security risk. The phishing incident at Eastern Valley Hospital caused by a staff member unknowingly clicking a fake login link is proof that untrained users can easily become gateways for cyber attackers.

A security framework is only as effective as the people who follow it. Therefore, building a culture of security awareness is just as important as installing firewalls or antivirus software.

6.2 Training Needs Identified

From interviews and the security audit, the following knowledge gaps were observed among staff:

- Inability to recognize phishing emails or suspicious links
- Weak password habits (e.g., reusing credentials, writing them down)
- Lack of understanding of data privacy rules and patient confidentiality
- Unawareness of how or where to report incidents
- No familiarity with new tools like MFA or USB device blocking

6.3 Awareness Program Design

The hospital's Security Awareness Program will be simple, engaging, and role-based. The content will be tailored to different groups (e.g., nurses, administrative staff, IT team) and delivered in short, digestible formats.

Training Modules

1. **Cybersecurity Basics for Healthcare Workers**
    - Why security matters in hospitals
    - How attacks like phishing happen
2. **Recognizing and Avoiding Threats**
    - How to spot suspicious emails, websites, and files
    - Real examples of phishing and ransomware
3. **Safe Password and Login Practices**
    - Creating strong passwords
    - How to use and set up MFA
4. **Protecting Patient Data**

- Legal obligations under Ghana's Data Protection Act
- Ethical principles of confidentiality and consent

5. **Reporting Incidents**
    - How to report suspicious activity or data breaches
    - Contact details and step-by-step process

6.4 Training Delivery Method

To accommodate busy schedules, training will be modular and short (15–20 minutes per session), using:

Format	Details
On-site sessions	Department-level mini-workshops every 2 weeks
Printed materials	Quick guides, posters, "DOs & DON'Ts" at workstations
Digital resources	PDF infographics and tip sheets via hospital email
Simulated emails	Phishing simulations to test user alertness

6.5 Implementation Timeline

Week	Activity
1	Launch campaign: "Your Role in Security"
2–3	Staff training begins (2 departments per week)
4	First phishing simulation (GoPhish tool)
6	Posters, guides, and feedback collection
8+	Quarterly refreshers and new topics

6.6 Measuring Effectiveness

To ensure the program is actually making a difference, the following methods will be used:

- **Pre- and post-training quizzes**
- **Phishing test click rates** (tracked over time)

CHAPTER 7

IMPLEMENTATION ROADMAP

7.1 Overview of Rollout Strategy

To avoid disruption to clinical services and reduce staff resistance, implementation will be carried out in **four practical phases**. Each phase is aligned with the hospital's budget, staff availability, and technical capacity.

This phased approach ensures that technical, administrative, and human elements are addressed in a logical order.

7.2 Implementation Phases and Activities

Phase	Timeline	Key Activities
Phase 1: Foundation & Compliance	Weeks 1–2	- Appoint part-time Data Protection Officer (DPO)
Phase 2: Technical Controls Setup	Weeks 3–5	- Install pfSense firewall - Deploy Bitdefender antivirus to all endpoints - Enable Google MFA for email and EMR - Configure USB control policies - Set up RBAC in EMR system
Phase 3: Awareness & Training	Weeks 6–7	- Conduct in-person departmental training sessions - Distribute guides and post infographics - Run phishing simulation (GoPhish)
Phase 4: Monitoring & Maintenance	Week 8 onward	- Begin monthly incident log reviews - Collect training feedback - Plan for quarterly refresher training - Prepare for internal security audit in 6 months

7.3 Resources and Budget Summary

Resource	Description
Personnel	IT Lead, DPO (part-time), Admin support staff
Hardware	pfSense-capable PC or appliance (for firewall)
Software Tools	Bitdefender licenses, VeraCrypt, GoPhish
Training Materials	Posters, PDFs, PowerPoint slides
External Support	Optional cybersecurity consultant (for setup)

7.4 Timeline Chart (8-Week Plan)

Week	Activity Snapshot
1	DPO appointed, security policies reviewed
2	Staff notified, policies signed
3	Firewall and antivirus setup begins
4	MFA and USB control configured
5	EMR roles assigned and access policies finalized
6	Staff training workshops begin
7	First phishing simulation, training materials distributed
8	Launch of monitoring program, review feedback and next steps

CHAPTER 8

CONCLUSIONS AND RECOMMENDATIONS

Summary of Findings

This project examined Eastern Valley Hospital's response to a phishing attack and assessed its overall information security posture. The investigation revealed major gaps in policy, awareness, and technical safeguards. A comprehensive security framework has been proposed to mitigate risks, ensure compliance with legal standards, and foster a security-conscious culture.

Key Recommendations

1. **Policy and Governance**
    - Approve and enforce clear policies for access control, data handling, acceptable use, and incident response.
    - Appoint a Data Protection Officer (DPO) and form a Security Review Committee.
2. **Technical Controls**
    - Deploy pfSense firewall, Bitdefender antivirus, and VeraCrypt for encryption.
    - Enforce MFA for Google Workspace and EMR systems.
    - Configure role-based access control in all key systems.
3. **User Awareness and Training**
    - Implement a security training program focused on phishing, password hygiene, and data handling.
    - Conduct quarterly refresher training and regular phishing simulations.
4. **Compliance and Ethics**
    - Register with the Ghana Data Protection Commission.
    - Ensure patients' privacy rights and ethical data handling are respected in all departments.
5. **Phased Rollout**
    - Use the proposed 8-week implementation roadmap to gradually introduce controls without disrupting hospital operations.

REFERENCES

Ghana Data Protection Commission. (2012). *Data Protection Act, 2012 (Act 843)*. https://www.dataprotection.org.gh

European Union. (2016). *General Data Protection Regulation (GDPR)*. https://gdpr.eu

pfSense. (2024). *Open Source Firewall*. https://www.pfsense.org

Bitdefender. (2024). *GravityZone Business Security*. https://www.bitdefender.com/business

VeraCrypt. (2024). *Disk Encryption Software*. https://www.veracrypt.fr

Google Workspace. (2024). *2-Step Verification Help*. https://support.google.com/accounts/answer/185839

ISO/IEC. (2013). *ISO/IEC 27001:2013 Security Techniques*. International Organization for Standardization

GoPhish. (2024). *Phishing Simulation Toolkit*. https://getgophish.com

Schneier, B. (2015). *Data and Goliath*. W. W. Norton & Company