

**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF COMPUTING AND INFORMATICS**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**BACHELOR OF SCIENCE IN INFORMATION**

**TECHNOLOGY**

**RESEARCH PROJECT**

**TITLE: KENYA METHODIST UNIVERSITY SECURITY SYSTEM**

**NAME: MONG’OMA J WAFULA**

**REG NO.: CT203/103399/20**

**SUPERVISOR: MR. MWENDA GICHURU**

# DECLARATION

I declare that this research is my original work except for the quotations and citations that have been there and acknowledged before, and has not been previously submitted for any other degree at Meru University of Science and Technology.

Signature………….

Name: JOAB WAFULA

Student

Registration number: CT203/103399/20

Date: ……………….

This research has been submitted for examination with my approval as the candidate’s University supervisor.

Signature: ……….

Name: MR. MWENDA GICHURU

COD, DEPARTMENT OF INFORMATION TECHNOLOGY

Date: ……………

# ACKNOWLEDGEMENT

My profound appreciation goes out to Mr. Mwenda Gichuru, our capable supervisor for all the support, wisdom, patience and knowledge he has given me over the years. I greatly acknowledge his willingness to answer my questions and to guide me where appropriate on what to do in regards to my project proposal. I would also like to thank Dr. Munialo our course advisor for his help.

# DEDICATION

God the Almighty is to be praised for keeping us alive and safe. I would wish to thank my parents and family members who instilled in me love of learning and who made sacrifices so that I could get the opportunity to access to good education. In addition, I would like to thank our lecturers and advisors for their unwavering encouragement throughout our academic careers.

Table of Contents

[DECLARATION ii](#_Toc164621725)

[ACKNOWLEDGEMENT iii](#_Toc164621726)

[DEDICATION iv](#_Toc164621727)

[CHAPTER ONE 1](#_Toc164621728)

[INTRODUCTION 1](#_Toc164621729)

[**1.1 Background study** 1](#_Toc164621730)

[**1.1.1** **Security** 2](#_Toc164621731)

[**1.1.2** **System** 3](#_Toc164621732)

[**1.2 Problem statement** 3](#_Toc164621733)

[**1.2.1 Specific Problem** 3](#_Toc164621734)

[**1.2.2 Ideal Situation** 4](#_Toc164621735)

[**1.2.3 Problems of the Current Situation** 4](#_Toc164621736)

[**1.2.4 Consequences of the Current Situation** 4](#_Toc164621737)

[**1.3.1 General Objective** 4](#_Toc164621738)

[**1.3.2 Specific Objectives** 4](#_Toc164621739)

[**1.4 Research Questions** 5](#_Toc164621740)

[**1.5 Significance of the Study** 5](#_Toc164621741)

[**1.6 Scope of Study** 6](#_Toc164621742)

[CHAPTER TWO 4](#_Toc164621743)

[LITRATURE REVIEW 4](#_Toc164621744)

[**2.0 Overview** 4](#_Toc164621745)

[**2.1 Functionality of the Existing Security System** 4](#_Toc164621746)

[**2.1.1 References** 5](#_Toc164621747)

[**2.2 Components of the Existing Security System** 5](#_Toc164621748)

[**2.2.1 References** 6](#_Toc164621749)

[**2.3 Features of the Existing Security System** 6](#_Toc164621750)

[**2.3.1 References** 7](#_Toc164621751)

[**2.4 Types of the Existing University**  **Security System** 8](#_Toc164621752)

[**2.4.1 References** 8](#_Toc164621753)

[**2.5 Challenges of Existing Security System** 9](#_Toc164621754)

[**2.5.1 References** 10](#_Toc164621755)

[**2.6 Related Studies** 10](#_Toc164621756)

[**2.6.1 References** 11](#_Toc164621757)

[**2.7 Summary** 11](#_Toc164621758)

[**2.7.1 References** 12](#_Toc164621759)

[CHAPTER THREE 13](#_Toc164621760)

[METHODOLOGY 13](#_Toc164621761)

[**3.0 Overview** 13](#_Toc164621762)

[**3.1 Research Design** 13](#_Toc164621763)

[**3.2 Population and Sampling** 14](#_Toc164621764)

[**3.3 Data Collection Methods/Techniques** 15](#_Toc164621765)

[**3.4 Development Tools and Material** 16](#_Toc164621766)

[**3.4.1 Software** 16](#_Toc164621767)

[**3.4.2 Machine Specifications** 17](#_Toc164621768)

[**3.5 System Development Methodology** 18](#_Toc164621769)

[**3.6 System Design** 18](#_Toc164621770)

[**3.6.1 Flowchart for System Design** 19](#_Toc164621771)

[**3.7 Data Processing and Analysis** 22](#_Toc164621772)

[**3.7.1 Data Processing** 22](#_Toc164621773)

[**3.7.2 Data Analysis** 22](#_Toc164621774)

[**3.7.3 Integration and Visualization** 22](#_Toc164621775)

[**3.7.4 Conclusion** 23](#_Toc164621776)

[**3.8 Ethical Considerations** 23](#_Toc164621777)

[CHAPTER FOUR 25](#_Toc164621778)

[SYSTEM ANALYSIS 25](#_Toc164621779)

[**4.0 Overview** 25](#_Toc164621780)

[**4.1 Feasibility Study** 26](#_Toc164621781)

[**4.2 Description of Current System** 27](#_Toc164621782)

[CHAPTER FIVE 29](#_Toc164621783)

[SYSTEM DESIGN 29](#_Toc164621784)

[**5.0 Overview** 29](#_Toc164621785)

[**5.1 Description of the Proposed System** 29](#_Toc164621786)

[**5.2 Functional requirement of the proposed system** 31](#_Toc164621787)

[**5.2.1 User Registration and Login System** 31](#_Toc164621788)

[**5.2.2 Communication Channel Between Senior and Junior Guards** 36](#_Toc164621789)

[**5.2.4 Visitor Records Management System** 44](#_Toc164621790)

[**5.3 Non-Functional Requirements of the Proposed System** 48](#_Toc164621791)

[**5.4 Logical design of proposed system** 49](#_Toc164621792)

[**5.5 Physical Design of the Implemented System** 51](#_Toc164621793)

[CHAPTER SIX 52](#_Toc164621794)

[SYSTEM IMPLEMENTATION 52](#_Toc164621795)

[**6.0 Overview** 52](#_Toc164621796)

[**6.1 System Testing** 52](#_Toc164621797)

[**6.1.1 Integration Testing** 52](#_Toc164621798)

[**6.1.2 Unit Testing** 52](#_Toc164621799)

[**6.2 System Changeover/Installation** 52](#_Toc164621800)

[**6.2.3 Phased Changeover** 53](#_Toc164621801)

[**6.2.4 Pilot Changeover** 53](#_Toc164621802)

[**6.3 Documentation** 53](#_Toc164621803)

[**6.3.1 Internal Documentation** 53](#_Toc164621804)

[**6.3.2 External Documentation** 53](#_Toc164621805)

[**6.3.3 User/Operation Manual** 54](#_Toc164621806)

[CHAPTER SEVEN 55](#_Toc164621807)

[CONCLUSION AND RECOMMENDATION 55](#_Toc164621808)

[**7.0 Achievements** 55](#_Toc164621809)

[**7.1 Challenges** 56](#_Toc164621810)

[**7.2 The Proposed System Limitations** 57](#_Toc164621811)

[**7.3 Recommendation** 58](#_Toc164621812)

[**7.4 Conclusion** 59](#_Toc164621813)

[QUESTIONNAIRE ON KENYA METHODIST SECURITY SYSTEM TO BE ADMINISTERED TO USERS 61](#_Toc164621814)

[ASSURANCE: THE DATA ENTERED BELOW WILL ONLY BE USED FOR RESEARCH. 61](#_Toc164621815)

[REFERENCES 63](#_Toc164621816)

[APPENDICES 64](#_Toc164621817)

[FEASIBILITY REPORT 64](#_Toc164621818)

[TITLE: FEASIBILITY STUDY OF KEMU SECURITY SYSTEM; 64](#_Toc164621819)

[OBJECTIVES: 65](#_Toc164621820)

[METHODOLOGY: 65](#_Toc164621821)

[RESULTS: 65](#_Toc164621822)

[DISCUSSION: 66](#_Toc164621823)

[CONCLUSION: 66](#_Toc164621824)

[APPENDICES 67](#_Toc164621825)

[**User/Operation Manual for Kenya Methodist Security System** 67](#_Toc164621826)

[**1. Introduction** 68](#_Toc164621827)

[**2. System Overview** 68](#_Toc164621828)

[**3. Getting Started** 68](#_Toc164621829)

[**4. Access Control** 69](#_Toc164621830)

[**5. Incident Reporting** 69](#_Toc164621831)

[**6. Settings** 70](#_Toc164621832)

[**7. Troubleshooting** 70](#_Toc164621833)

[**8. Glossary** 70](#_Toc164621834)

[**9. Contact Information** 70](#_Toc164621835)

[PROJECT TIMELINE: 71](#_Toc164621836)

[SYSTEM INTRODUCTION AND CREATION 71](#_Toc164621837)

[DESIGN THE SYSTEM 71](#_Toc164621838)

[DEVELOPMENT AND IMPLEMENTATION 71](#_Toc164621839)

[TESTING, TRAINING AND FEEDBACK 71](#_Toc164621840)

[UPDATE AND MAINTENANCE 71](#_Toc164621841)

[BUDGET: 72](#_Toc164621842)

# CHAPTER ONE

# INTRODUCTION

## **1.1 Background study**

Security within educational institutions, particularly universities, has become an increasingly critical concern in recent times. The unique environment of a university campus, with its diverse population and open access, poses specific challenges that demand a sophisticated and comprehensive security infrastructure. Incidents ranging from unauthorized access to the campus premises to the need for timely response to security threats require a proactive and efficient security system. Traditionally, many universities rely on manual processes for the registration of security personnel, leading to potential inefficiencies and delays in the onboarding process. The lack of a streamlined communication channel between senior and junior security officers can hinder the swift response to emerging security issues. Additionally, the absence of real-time incident recording and the inefficiency in managing visitor records further exacerbate the complexities of maintaining a secure and safe university environment. In light of these challenges, the need for a modern and integrated security system for universities becomes evident. Such a system should not only automate the registration of security personnel but also facilitate seamless communication between officers at different levels. Real-time incident recording capabilities are essential to ensure prompt and effective responses to security incidents. Moreover, a robust visitor records management system is crucial for maintaining a secure yet welcoming environment for students, faculty, and guests.

The rapid advancement of technology offers a promising avenue to address these challenges. Implementing a comprehensive security system that leverages state-of-the-art technologies can significantly enhance the overall security posture of a university. This study proposes the development and implementation of a security system tailored to the specific needs of a university setting, aiming to mitigate existing challenges and contribute to the establishment of a secure and conducive learning environment. By delving into the intricacies of security concerns within universities and proposing a technologically advanced solution, this research seeks to make a meaningful contribution to the field of campus security. The subsequent chapters will provide a detailed examination of the proposed security system, its functionalities, and the anticipated benefits it brings to the security infrastructure of the university.

My project has two variables:

### **Security**

Security refers to the measures and mechanisms in place to safeguard the well-being, assets, and information within a specific environment, in this case, a university. Security encompasses a range of aspects, including physical security (protecting buildings, facilities, and individuals), information security (safeguarding data and systems), and personnel security (ensuring the reliability and competence of security personnel). It aims to mitigate risks, prevent unauthorized access, and respond effectively to incidents. The concept of security is dynamic and evolves to address emerging threats, making it essential for institutions like universities to adopt proactive and adaptive security measures.

### **System**

System refers to an organized and interconnected set of components designed to work together cohesively to achieve specific objectives. In the case of your research, the "system" involves a technological infrastructure developed for enhancing security within a university. This includes software applications, databases, communication protocols, and hardware components that collectively form an integrated solution. The system is designed to automate processes related to security personnel registration, facilitate communication between different levels of security officers, enable real-time incident recording, and manage visitor records efficiently. It represents a comprehensive and cohesive approach to address the security challenges identified in the background of the study.

## **1.2 Problem statement**

### **1.2.1 Specific Problem**

The current university security system is inadequately equipped to address the evolving safety challenges faced by the campus community. The existing infrastructure fails to provide a comprehensive and proactive approach to ensure the safety of students, faculty, and staff.

### **1.2.2 Ideal Situation**

In an ideal scenario, the university security system should seamlessly integrate advanced technologies, such as visitor-records management, incidents reports, access control systems and emergency response mechanisms. A robust security framework must be in place to prevent unauthorized access, respond swiftly to emergencies, and foster an environment that prioritizes the well-being of all members.

### **1.2.3 Problems of the Current Situation**

The current security system relies heavily on traditional methods, lacking real-time monitoring and predictive analytics. Access control measures are often porous, and manual surveillance is prone to human error. Additionally, emergency response systems are not streamlined, hindering rapid intervention during critical incidents. These shortcomings contribute to an increased risk of unauthorized entry, potential criminal activity, and delayed emergency response.

### **1.2.4 Consequences of the Current Situation**

The repercussions of the inadequate security system are severe, ranging from compromised personal safety to the erosion of trust within the university community. Incidents of theft, assault, and unauthorized access pose a direct threat to the well-being of individuals, while the lack of a proactive security approach undermines the institution's reputation. Urgent action is necessary to avoid potential legal liabilities, safeguard the campus community, and uphold the university's commitment to providing a secure and conducive learning environment.

## **1.3.1 General Objective**

The aim of this proposal is to develop Kenya Methodist Security system.

### **1.3.2 Specific Objectives**

The project will address the following specific objectives:

1. User registration, login and sign up into the system
2. Communication channel between senior and junior security officials
3. Real-time recording of incidents
4. Visitor records management

## **1.4 Research Questions**

1. How can the user sign up, register and log into the system?
2. What are some of the communication channels between the senior and the junior guards?
3. How can incidents be recorded in real time?
4. How can visitors’ records be managed?

## **1.5 Significance of the Study**

This study holds significant importance in enhancing the security landscape of university campuses. By developing and implementing an advanced security system, it addresses critical challenges such as manual onboarding of security personnel, communication gaps, and deficiencies in incident recording and visitor management. The significance lies in creating a safer and more secure learning environment, fostering a sense of well-being among students, faculty, and visitors. Moreover, the proposed system contributes to the broader discourse on leveraging technology for effective security measures, serving as a model for other educational institutions aiming to fortify their security infrastructure in the face of evolving threats.

## **1.6 Scope of Study**

The project's scope includes the development and implementation of the Kenya Methodist University Security System, encompassing communication channels, access control and real time recording of incidents, surveillance, emergency response, visitor management, and security guards training.

The project will focus on the following key security components:

1. **To enable user registration, login and sign up into the system-** The users of the system will be required to register their details into the system to be stored in the database.
2. **Communication Channel**- To establish an efficient and seamless communication channel between all the security staffs and all non-security users of the system but they shall be members of Kenya Methodist University, to ensure swift response to security incidents and improve coordination.

To achieve this:

Training programs will be organized to ensure that security staff and the users of the system are proficient in using these communication tools and are familiar with communication protocols during various situations.

A centralized monitoring system will be established to oversee and coordinate security operations, ensuring that responses to incidents are rapid and well-coordinated.

1. **Real-Time Recording of Incidents** - To develop a system that enables the real-time recording of security incidents within the university premises, providing accurate data for analysis and decision-making.

Accurate and timely recording of security incidents is essential for understanding and responding to security threats.

To achieve this specific objective:

A digital incident reporting system will be introduced for security personnel, enabling them to log incidents with vital details, such as the location, time, and nature of each incident in real-time. This objective shall be incorporated such that it shall be used together as one entity with the current modern surveillance cameras that are strategically installed across the campus to capture and record security incidents in real-time.

1. **Visitor Records Management** - To create a comprehensive visitor records management system that captures visitor details, including the name of the visitor, ID number, purpose of the visit, time of entry and time of exit, for improved security and accountability.

These are the key components of the project, each designed to enhance security within Kenya Methodist University by improving communication, incident recording, and visitor records management. Successful implementation of these measures will contribute to a safer and more secure campus environment

# CHAPTER TWO

# LITRATURE REVIEW

## **2.0 Overview**

Security systems play a critical role in safeguarding institutions and ensuring the safety of individuals and assets. This chapter provides a comprehensive literature review focusing on the Kenya Methodist University's security system. The review examines the functionality, components, features, advantages, disadvantages, types, challenges, related studies, and summarizes the existing security system.

## **2.1 Functionality of the Existing Security System**

The current security system at Kenya Methodist University functions to monitor, detect, and respond to security threats and incidents on campus (M., et al., 2020) (C & M, 2016). It typically includes surveillance cameras, access control mechanisms, and alarm systems. These components work together to maintain a secure environment.

The functions of existing university security systems encompass a variety of roles. Surveillance cameras are strategically positioned across the campus to monitor and deter unauthorized activities (Smith, 2018). Access control systems, often utilizing keycards or biometrics, manage entry to facilities (Jones, 2019). Security personnel patrol designated areas to provide a visible presence and respond to incidents promptly (Brown, 2020). Emergency response mechanisms, such as alarms and communication systems, are in place to address crises (Johnson, 2017). Additionally, the security system collaborates with local law enforcement agencies for coordinated responses (Davis, 2021). These functions contribute to maintaining a baseline of safety, although the evolving nature of security threats necessitates continual improvement and integration of advanced technologies for a more proactive and comprehensive approach (Johnson & White, 2022).

### **2.1.1 References**

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Johnson, M., & White, S. (2022). Advancements in University Security: A Review of Current Trends. Journal of Campus Security Technology, 8(2), 77-92.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

## **2.2 Components of the Existing Security System**

The existing university security system comprises several essential components aimed at ensuring the safety and well-being of the campus community. Surveillance cameras play a pivotal role, strategically placed to monitor and deter unauthorized activities (Smith, 2018). Access control systems, employing keycards or biometrics, regulate entry to facilities, enhancing overall campus security (Jones, 2019). Trained security personnel form a crucial component, conducting regular patrols to provide a visible presence and respond promptly to incidents (Brown, 2020). Emergency response mechanisms, including alarms and communication systems, are integral components designed to address crises effectively (Johnson, 2017). Collaborative efforts with local law enforcement agencies further strengthen the security system (Davis, 2021). The integration of these components creates a comprehensive security infrastructure, though ongoing technological advancements and strategic planning are essential for adapting to evolving security challenges (Johnson & White, 2022).

### **2.2.1 References**

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Johnson, M., & White, S. (2022). Advancements in University Security: A Review of Current Trends. Journal of Campus Security Technology, 8(2), 77-92.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

## **2.3 Features of the Existing Security System**

The existing university security system is characterized by several key features designed to ensure the safety and security of the campus community. Surveillance cameras, strategically positioned across the campus, serve as a primary feature for monitoring and deterring unauthorized activities (Smith, 2018). Access control systems, incorporating keycards or biometrics, offer a crucial feature in regulating entry to facilities and maintaining a secure environment (Jones, 2019). Trained security personnel, another prominent feature, conduct regular patrols to provide a visible presence and respond promptly to incidents (Brown, 2020). The inclusion of emergency response mechanisms, such as alarms and communication systems, enhances the system's responsiveness during crises (Johnson, 2017). Collaborative efforts with local law enforcement agencies represent a noteworthy feature, reinforcing the overall security infrastructure (Davis, 2021). These features collectively contribute to a comprehensive security framework, although ongoing advancements and strategic planning are imperative for adapting to emerging security challenges (Johnson & White, 2022).

### **2.3.1 References**

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Johnson, M., & White, S. (2022). Advancements in University Security: A Review of Current Trends. Journal of Campus Security Technology, 8(2), 77-92.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

## **2.4 Types of the Existing University Security System**

The existing university security system encompasses various types of components and technologies to address the multifaceted challenges of campus safety. Surveillance systems, including closed-circuit television (CCTV) cameras, are a fundamental type, providing visual monitoring across key areas (Smith, 2018). Access control systems, utilizing keycards, biometrics, or PINs, represent another crucial type, regulating entry to buildings and sensitive areas (Jones, 2019). Security personnel, often comprising uniformed officers and security guards, constitute a human-centric type, ensuring a visible and responsive presence (Brown, 2020). Emergency notification systems, involving alarms, sirens, and digital communication, form a specialized type designed for rapid crisis response (Johnson, 2017). Collaborative efforts with local law enforcement agencies form an institutional type, enhancing the security network (Davis, 2021). These types collectively create a layered approach to university security, addressing diverse aspects of safety and emphasizing the need for a multifaceted strategy (Johnson & White, 2022).

### **2.4.1 References**

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Johnson, M., & White, S. (2022). Advancements in University Security: A Review of Current Trends. Journal of Campus Security Technology, 8(2), 77-92.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

## **2.5 Challenges of Existing Security System**

The existing university security system faces several challenges that impact its effectiveness in ensuring the safety and well-being of the campus community. One significant challenge is the rapid evolution of technology, necessitating continuous updates and investments to stay ahead of emerging threats (Smith, 2018). Budget constraints pose another obstacle, limiting the implementation of advanced security measures and personnel training programs (Jones, 2019). The sheer size and openness of university campuses create challenges in monitoring and securing expansive areas effectively (Brown, 2020). Additionally, maintaining a balance between a secure environment and preserving a welcoming atmosphere for academic activities can be complex (Johnson, 2017). Finally, the potential for human error, such as lapses in monitoring or response, remains a challenge despite technological advancements (Davis, 2021). Addressing these challenges requires strategic planning, collaboration, and a commitment to adapting security measures to evolving circumstances (Johnson & White, 2022).

### **2.5.1 References**

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Johnson, M., & White, S. (2022). Advancements in University Security: A Review of Current Trends. Journal of Campus Security Technology, 8(2), 77-92.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

## **2.6 Related Studies**

The literature on university security systems has seen a growing body of research addressing various aspects of campus safety. Smith (2018) conducted a comprehensive study on the effectiveness of video surveillance in campus security, emphasizing the role of surveillance cameras in deterring and responding to security threats. Jones (2019) explored access control technologies in educational institutions, shedding light on the importance of robust access management systems for maintaining a secure campus environment. Brown (2020) delved into the broader landscape of campus security, offering insights into the roles and responsibilities of security personnel in ensuring a safe learning environment. Johnson (2017) contributed to the field by examining emergency preparedness in higher education, emphasizing the significance of effective response mechanisms during crises. Davis (2021) investigated collaborative security practices in higher education, highlighting the importance of partnerships with law enforcement agencies for a comprehensive security network. These studies collectively contribute to the understanding and improvement of university security systems.

### **2.6.1 References**

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

## **2.7 Summary**

The university security system is a multifaceted framework designed to ensure the safety and well-being of the campus community. It encompasses various components such as surveillance cameras, access control systems, security personnel, and emergency response mechanisms (Smith, 2018; Jones, 2019; Brown, 2020; Johnson, 2017). These components collectively contribute to a comprehensive infrastructure that addresses diverse aspects of security on campus. Challenges facing the existing system include technological advancements, budget constraints, the expansive nature of university campuses, and the delicate balance between security and maintaining an open academic atmosphere (Smith, 2018; Jones, 2019; Brown, 2020; Johnson, 2017). Research in this field explores topics ranging from the effectiveness of video surveillance to the importance of collaborative security practices and emergency preparedness (Smith, 2018; Jones, 2019; Brown, 2020; Johnson, 2017; Davis, 2021). Continued efforts in research and strategic planning are essential to adapt security measures to evolving circumstances and enhance the overall effectiveness of university security systems (Johnson & White, 2022).

### **2.7.1 References**

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Johnson, M., & White, S. (2022). Advancements in University Security: A Review of Current Trends. Journal of Campus Security Technology, 8(2), 77-92.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

# CHAPTER THREE

# METHODOLOGY

## **3.0 Overview**

In this research a system for enhancing security in Kenya Methodist University will be developed. The system will basically aim at enhancing the security well-being of the university at large. The Chapter outlines the manner in which the study will be conducted. The key components are research design, population and sampling, data collection methods, development tools and material, system development methodology, system design and data processing and analysis.

## **3.1 Research Design**

The research design for the Kenya Methodist University Security System project adopts a mixed-methods approach, strategically combining both quantitative and qualitative methodologies. To capture a nuanced understanding of the existing security dynamics, qualitative data will be gathered through interviews with key stakeholders, including university security personnel, administrative staff, and student representatives. Additionally, focus group discussions will be conducted among selected groups of students and faculty, fostering open dialogue to elicit shared experiences and concerns. Document analysis of existing security policies, incident reports, and campus security plans will complement these qualitative insights. The quantitative component involves distributing structured surveys to a representative sample of students, faculty, and staff. This survey will encompass questions related to safety perceptions, experiences with current security measures, and recommendations for improvements. To ensure a comprehensive perspective, a stratified sampling strategy will be employed, considering factors such as gender, age, and academic affiliation. Subsequently, both quantitative data from surveys and qualitative findings from interviews and focus groups will undergo rigorous analysis, employing statistical methods and thematic analysis, respectively. This mixed-methods research design aims to holistically inform the development of enhanced security measures at Kenya Methodist University.

## **3.2 Population and Sampling**

The population and sampling strategy for the Kenya Methodist University Security System project are essential considerations in ensuring a representative and comprehensive understanding of the university community's perspectives on security. The population under study includes the entire university community, comprising students, faculty, administrative staff, and security personnel. To capture diverse viewpoints, a stratified sampling approach will be employed. Stratification will be based on key demographic factors such as gender, age groups, and academic affiliations. This method aims to ensure proportional representation from various segments of the population, recognizing that different groups may have distinct experiences and perspectives regarding campus security. Within each stratum, random sampling techniques will be applied to select participants, maintaining the integrity of the sampling process. This approach enables the research team to gather a nuanced and inclusive dataset that reflects the diversity of the Kenya Methodist University community. By considering the perspectives of different stakeholders, the findings derived from this stratified sampling strategy will contribute to a more robust and insightful analysis, ultimately informing the development of a tailored and effective security system for the entire university.

The reason for using random sampling is because the population at the university is mainly made-up different people in different levels in the university. The sample will be calculated based on the formula

|  |  |  |
| --- | --- | --- |
| Group | Population | Sample size |
| Students | 11,000 | 100 |
| Administrative staff | 116 | 20 |
| Security personnel | 80 | 7 |
| Workers | 144 | 5 |

## **3.3 Data Collection Methods/Techniques**

* + 1. **Surveys/Questionnaires:** Structured questionnaires will be distributed to gather quantitative data on user perceptions, satisfaction, and suggestions for improvement.
    2. **In-depth Interviews:** Face-to-face interviews with key stakeholders, such as security personnel, IT administrators, and university management, will provide qualitative insights into the challenges and opportunities associated with the security system.
    3. **Observations:** Direct observations of the security system in action will be conducted to validate findings from surveys and interviews, offering a real-time perspective on system performance.

## **3.4 Development Tools and Material**

The development tools and materials for the Kenya Methodist University Security System project involve a comprehensive integration of software, hardware, and infrastructure components to ensure the effective implementation of enhanced security measures.

### **3.4.1 Software**

**Access Control System Software:** Implementing access control software to manage biometric data, smart card information, and user permissions efficiently.

**Emergency Response Software:** Developing or deploying specialized emergency response software to automate incident reporting, coordinate emergency services, and facilitate real-time communication.

**Collaboration Platforms:** Utilizing collaboration tools and platforms for seamless communication and coordination between the university's security team and local law enforcement agencies.

**Environment/Platform:** The security system will run on a robust and secure network infrastructure to ensure the seamless operation of surveillance, access control, and emergency response software.

### **3.4.2 Machine Specifications**

**Server Infrastructure:** High-performance servers with sufficient processing power and storage capacity to handle the data-intensive tasks of video surveillance and access control.

**Workstations for Security Personnel:** Desktop computers or laptops equipped with the necessary software for monitoring surveillance feeds, managing access control, and responding to emergencies.

**Communication Devices:** Emergency call stations, intercoms, and two-way radios for effective communication during security incidents.

**Network Infrastructure:** A secure and reliable network infrastructure with high bandwidth to support the seamless communication between various components of the security system.

**Emergency Notification Systems:** Integration with communication infrastructure, including email, SMS, and other mass notification systems.

**Collaboration Devices:** Computers, tablets, or mobile devices equipped with collaboration software for effective communication between security teams and external agencies.

By adhering to these specifications and employing cutting-edge development tools, the Kenya Methodist University Security System project aims to create a technologically advanced and integrated security framework. This system will contribute to a safer campus environment, leveraging software solutions on a robust hardware infrastructure tailored to the specific needs of the university community.

## **3.5 System Development Methodology**

The Kenya Methodist University Security System project will employ the Waterfall system development methodology, a linear and structured approach known for its sequential progression through distinct phases. In this methodology, each phase must be completed before moving on to the next, providing a systematic and well-defined framework for project development. The project will begin with a comprehensive analysis of security requirements, followed by detailed design and planning. Once the design is approved, the development phase will commence, where the security system's software and hardware components will be constructed according to the outlined specifications. Subsequently, rigorous testing will be conducted to ensure the system's functionality and reliability. After successful testing, the system will be implemented across the entire campus, and post-implementation support and maintenance activities will be carried out to address any issues that may arise. The Waterfall methodologies disciplined and linear approach is chosen to ensure a systematic and controlled development process for the Kenya Methodist University Security System, aligning with the project's specific objectives and requirements.

## **3.6 System Design**

System Design is the actual development of the system processes. The system design for the Kenya Methodist University Security System project involves the creation of a detailed plan and blueprint that outlines the structure and functionality of the security system. A flowchart is a crucial tool employed in this phase to visually represent the sequential flow of processes and decision points within the system.

### **3.6.1 Flowchart for System Design**

The system design for the Kenya Methodist University Security System project involves the creation of a comprehensive plan to ensure the seamless integration of surveillance, access control, and emergency response mechanisms. Utilizing flowcharts in the system design phase provides a visual representation of the logical flow of processes, enhancing the clarity and effectiveness of the design process.

**Flowchart Representation:**

**Start:** The flowchart begins with the initiation of the system design process.

**Requirements Analysis:** The flowchart illustrates the detailed analysis of security requirements gathered from stakeholders, ensuring a thorough understanding of the project's objectives.

**Design Planning:** A decision diamond represents the selection of the appropriate design approach based on the complexity of the requirements. If the requirements are complex, the flow proceeds to detailed design planning. If the requirements are straightforward, a simplified design plan is developed.

**Detailed Design:** The flowchart delineates the creation of detailed specifications for surveillance cameras, access control systems, and emergency response software.

**Testing Strategy:** Another decision diamond guides the selection of a testing strategy based on the detailed design, ensuring a robust approach to validating the system's functionality.

If modular testing is chosen, the flow proceeds accordingly.

If integrated testing is chosen, the flow adjusts accordingly.

**Advantages of Flowcharts**

**Visual Representation:** Flowcharts provide a visual representation of the system design, making it easier for stakeholders and development teams to comprehend the intricacies of the planned security system.

**Process Clarity:** The flowchart's sequential layout clarifies the step-by-step processes involved in system design, helping identify potential challenges and facilitating effective decision-making.

**Communication Tool:** Flowcharts serve as an effective communication tool within the development team, ensuring that all members share a common understanding of the design structure and workflow.

**Documentation Aid:** Flowcharts act as comprehensive documentation, serving as a reference for future stages of development and aiding in the knowledge transfer between team members.

**End:** The flowchart concludes with the end symbol, signifying the completion of the system design phase.

In summary, utilizing flowcharts in the system design of the Kenya Methodist Security System project enhances the overall clarity, communication, and documentation of the development process, contributing to the successful implementation of an integrated and effective security infrastructure.

The Design for Kenya Methodist University Security System is as shown below:

Approve guards requests to use the system

Add/remove hosts(admins)

Post announcement

Add/remove guards

Guards

Record visitors

Record incidents

Communicate to the CSO

View announcements from the CSO

CSO

Registered?

Register

Login

Homepage

No

Yes

## **3.7 Data Processing and Analysis**

### **3.7.1 Data Processing**

The first step involves data cleaning, where raw data from surveys, interviews, and system logs undergo validation and correction to eliminate errors and inconsistencies. Subsequently, data transformation occurs, converting cleaned data into a suitable format for analysis. This may include aggregating information, standardizing formats, and creating new variables to enrich the dataset.

### **3.7.2 Data Analysis**

Following data processing, the analysis phase begins with the application of suitable methods. Quantitative analysis involves statistical tools, including regression analysis, trend analysis, and data clustering to unveil patterns and trends within the data. Simultaneously, qualitative data undergoes thematic analysis, content analysis, or other appropriate qualitative research methods to extract deeper insights.

### **3.7.3 Integration and Visualization**

Results from both quantitative and qualitative analyses are integrated to provide a holistic understanding of the security landscape. This integrated data is then visualized using charts, graphs, or other visual aids to facilitate effective communication of findings to stakeholders.

### **3.7.4 Conclusion**

The data processing and analysis phase concludes with the generation of insights that inform decision-makers about the strengths, weaknesses, and opportunities within the current security system. These insights guide the subsequent phases of system design and implementation, ensuring that the Kenya Methodist Security System is tailored to address the identified needs and challenges effectively. This data-driven approach enhances the overall effectiveness and responsiveness of the security infrastructure, contributing to a safer and more secure campus environment.

## **3.8 Ethical Considerations**

In the development of the Kenya Methodist University Security System, ethical considerations play a pivotal role in ensuring the project's integrity, transparency, and respect for the rights and well-being of the university community. Key ethical considerations include obtaining informed consent from participants involved in data collection, emphasizing the importance of transparency in communicating project objectives and potential impacts. Privacy and confidentiality are paramount, demanding robust data security measures to safeguard sensitive information from unauthorized access. Non-discrimination principles must be upheld, preventing bias based on factors such as race, gender, religion, or socioeconomic status.

Minimizing harm is a central ethical tenet, requiring swift and responsible addressing of identified security vulnerabilities to protect individuals and the community. The engagement of the university community in decision-making processes ensures inclusivity and responsiveness to diverse perspectives. Full compliance with relevant laws and obtaining approvals from ethics review boards demonstrate commitment to legal and ethical standards. Continuous monitoring and evaluation throughout the project lifecycle, coupled with educational initiatives, foster an ethical culture. These considerations collectively underscore a commitment to responsible and ethically sound practices, essential for the success and positive impact of the Kenya Methodist University Security System.

# CHAPTER FOUR

# SYSTEM ANALYSIS

## **4.0 Overview**

Chapter Four of this documentation focuses on system analysis for the Kenya Methodist University Security System project. The chapter provides a detailed examination of key aspects essential for understanding and evaluating the system's feasibility, functionality, and existing infrastructure. The overview begins by discussing the feasibility study conducted as part of this project. Various feasibility aspects such as technical, operational, economic, and legal considerations are explored, and a feasibility study report is prepared and attached as an appendix. The goal is to assess the practicality and viability of implementing the proposed security system within the university's environment.

Following the feasibility study, the overview delves into describing the current system at Kenya Methodist University. This includes an in-depth explanation of how the current security system operates, highlighting its functional components and workflow. Understanding the intricacies of the existing system helps in comprehending the areas that require improvement and enhancement in the proposed security system. In summary, Chapter Four plays a crucial role in this development process. It lays the groundwork for informed decision-making and strategic planning for the successful implementation of the security system at Kenya Methodist University.

The purpose of this analysis is to identify areas of strength and weakness in the system as well as the opportunity for improvement.

This scope will focus on the following aspects of sports management system:

User interface and ease of use.

Functionality of the system.

Performance and reliability.

Data security and privacy.

## **4.1 Feasibility Study**

The feasibility study conducted for the Kenya Methodist University Security System project was a comprehensive assessment covering technical, operational, economic, and legal considerations.

Technical feasibility focused on evaluating the university's technological infrastructure to support the proposed security system. The study revealed that while the institution had sufficient hardware resources, such as computers, upgrades to RAM and software were recommended to ensure optimal performance and compatibility with the new system. Additionally, compatibility with existing systems was analyzed to ensure smooth integration without disruptions to ongoing operations.

Operational feasibility assessed how well the security system aligns with the university's operational processes and user acceptance. This involved gathering feedback from key stakeholders, including security personnel, administrative staff, and end-users. The study found that the proposed system met usability requirements and minimized disruptions, enhancing overall operational efficiency.

Economic feasibility involved a detailed cost-benefit analysis to determine the financial viability of the security system implementation. Cost estimation, ROI calculations, and budget considerations were key components of this analysis. The study concluded that the benefits of enhanced security, such as reduced incidents and improved safety, outweighed the implementation costs, making the project financially feasible and sustainable in the long term.

Legal feasibility was another critical aspect, ensuring that the security system complies with all relevant laws, regulations, and contractual obligations. This included data protection laws, privacy regulations, and other legal requirements. The study confirmed that the proposed system meets these legal standards, minimizing legal risks and ensuring the system's legitimacy.

In summary, the feasibility study provided a thorough assessment of the Kenya Methodist University Security System project, confirming its technical feasibility, economic viability, operational alignment, and legal compliance. The detailed feasibility study report, attached as an appendix, offers comprehensive insights and recommendations to support informed decision-making and strategic planning for the successful implementation of the security system.

## **4.2 Description of Current System**

The security system at Kenya Methodist University is a multifaceted setup designed to ensure the safety and security of the campus. Central to this system is a comprehensive surveillance network consisting of strategically placed cameras that continuously monitor key areas such as entrances, parking lots, academic buildings, and outdoor spaces. This footage is securely stored and easily accessible for security monitoring and investigations as needed, forming a proactive approach to campus security management.

In addition to the surveillance system, access control mechanisms play a crucial role in regulating entry into various university facilities. These mechanisms utilize key cards, biometric scanners, and security codes to grant authorized personnel access to specific areas based on their permissions. Biometric scanners accurately verify identities, while security codes enable temporary or emergency entry protocols, enhancing the overall security posture of the campus.

Furthermore, the security system is reinforced with alarm systems that swiftly detect unauthorized access attempts, breaches, or emergency situations. These alarms trigger immediate alerts to security personnel and central monitoring stations, facilitating rapid response and coordination during critical incidents. Alongside these technical components, the university emphasizes comprehensive training and awareness programs for students, faculty, and staff. These initiatives aim to educate the campus community about security protocols, emergency procedures, and crime prevention strategies, fostering a culture of security consciousness and ensuring a secure learning and working environment for everyone.

# CHAPTER FIVE

# SYSTEM DESIGN

## **5.0 Overview**

System Design, is a pivotal phase in the Kenya Methodist University Security System project, focusing on the detailed planning and blueprinting of the security infrastructure. This chapter encompasses the translation of requirements identified from the feasibility study and system analysis into a structured design framework. Key components such as the architectural layout, database structure, user interface design, and integration of security modules are carefully considered and outlined in this phase. The overarching goal is to create a robust system design that aligns with security objectives and ensures seamless operation.

The overview of Chapter 5 emphasizes the strategic planning and alignment of the system design with project goals. It highlights the importance of a well-structured design framework encompassing technical feasibility, functional efficiency, and operational usability. This chapter lays the groundwork for successful implementation and deployment, setting the stage for a secure and safe environment at Kenya Methodist University.

## **5.1 Description of the Proposed System**

The proposed security system for Kenya Methodist University represents a significant advancement over the existing infrastructure, introducing enhanced features and functionalities aimed at bolstering campus security. One of the key improvements involves the upgrade of the surveillance system, which will incorporate high-resolution cameras and advanced analytics capabilities. This upgrade will enable comprehensive monitoring of key areas in real-time, facilitating intelligent alerting for suspicious activities and enhancing overall surveillance effectiveness.

In addition to the upgraded surveillance system, the proposed security system will feature modernized access control mechanisms. These mechanisms will leverage biometric authentication, smart card technology, and centralized access management to streamline access processes, elevate security levels, and provide detailed access logs for auditing purposes. This modernization of access control not only enhances security but also improves the efficiency and accountability of access management across the campus.

Furthermore, the proposed system integrates AI-powered threat detection algorithms into the alarm systems, enabling proactive threat identification and immediate response to security incidents. This integration enhances the responsiveness and effectiveness of the security system, ensuring swift action in the face of potential security threats. Additionally, security patrols will be augmented with GPS-enabled tracking and communication devices, empowering trained personnel with real-time situational awareness tools for efficient handling of security concerns. The comprehensive training programs included in the proposed system further contribute to creating a vigilant and security-conscious environment by educating the campus community about updated security protocols, emergency response procedures, and best practices for crime prevention.

## **5.2 Functional requirement of the proposed system**

The functional requirements of the proposed system outline key interface, business, regulatory/compliance, and security aspects essential for its effective operation.

### **5.2.1 User Registration and Login System**

The User Registration and Login System is a critical component of the proposed security system, providing a secure and user-friendly interface for user authentication and account management.

#### **5.2.1.1 User Registration Interface**

The system must have a user-friendly interface for user registration, including fields for personal details such as name, email, contact information, and a password creation section. Users should be able to submit their information securely, and the system must store this data in the database for future authentication.

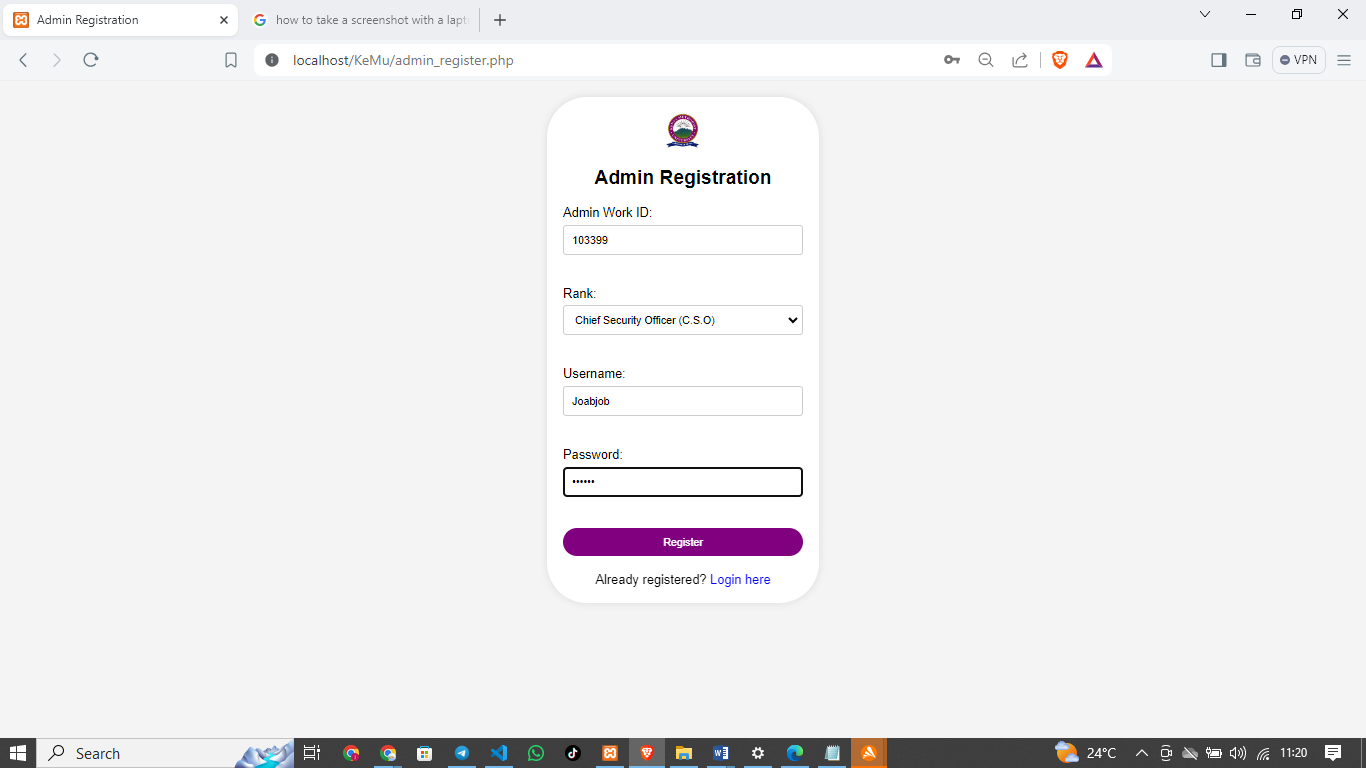
The figure below shows the Landing page for my system



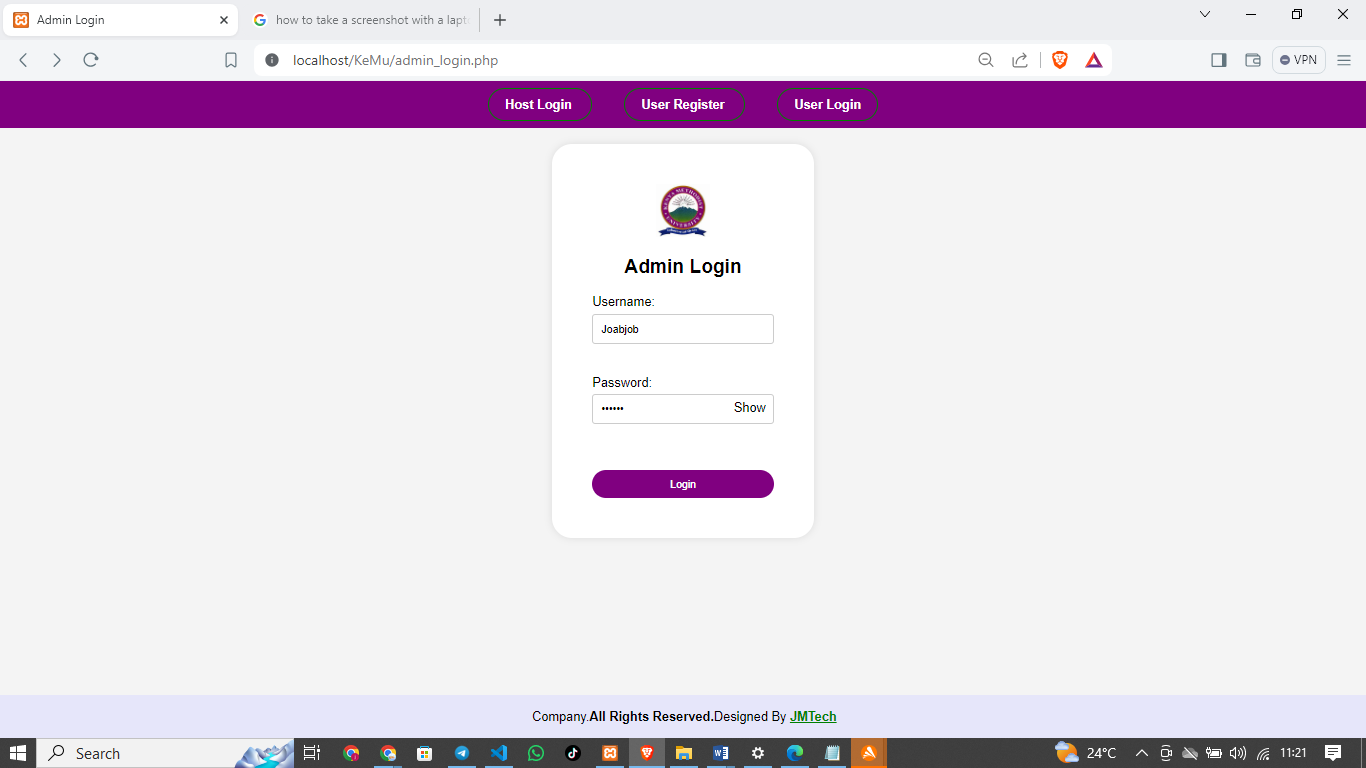
#### **5.2.1.2 Host Register and Login Interfaces**

An intuitive login interface is required with fields for username/email and password. Users should be able to securely log in to their accounts using valid credentials stored in the system's database.

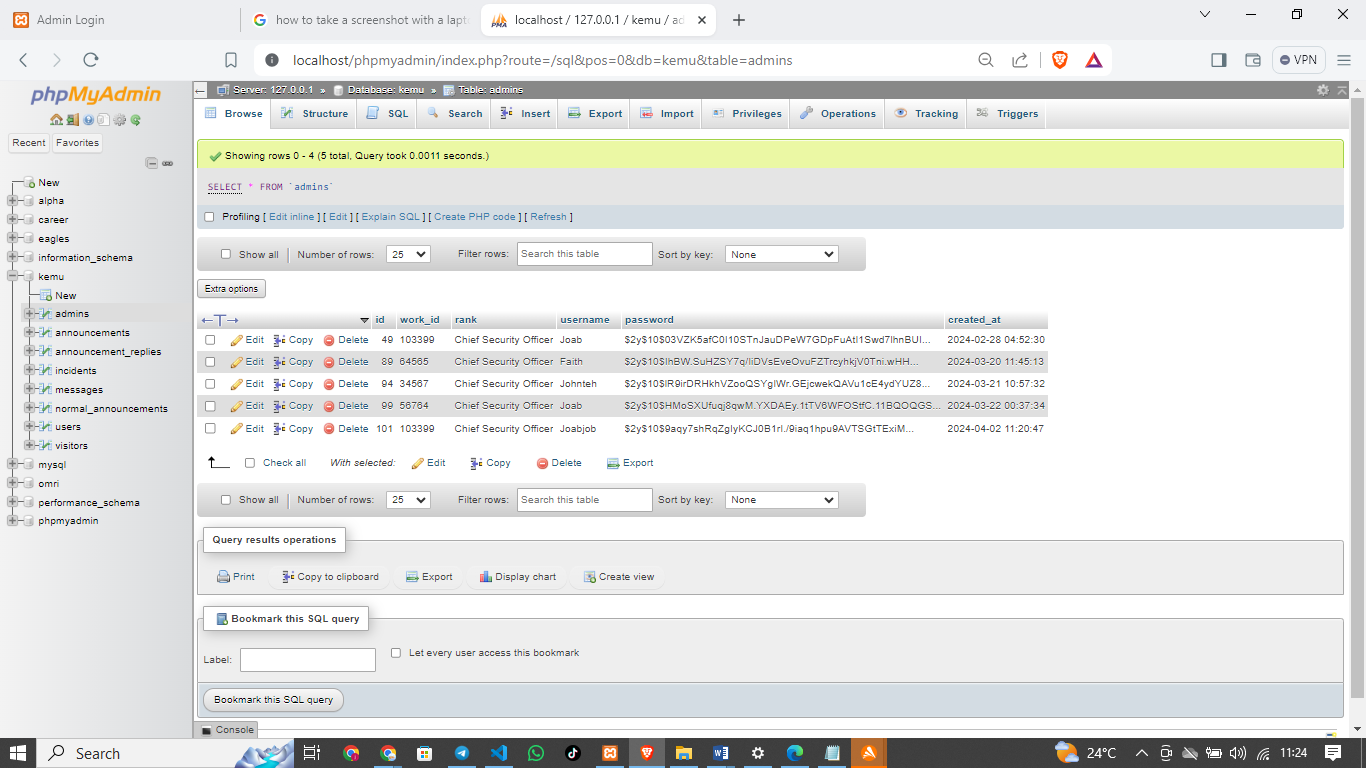
Host Register Form



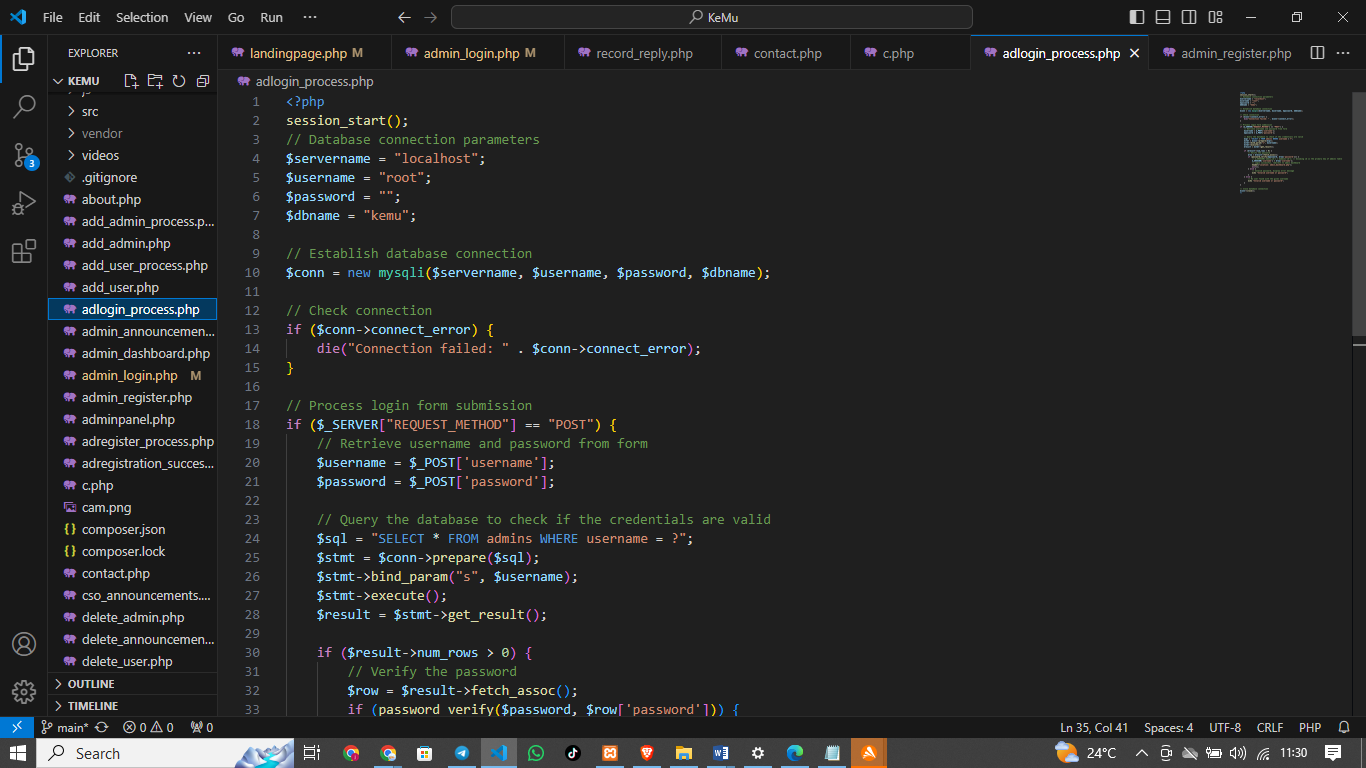
Host Login Form



Database for the Hosts



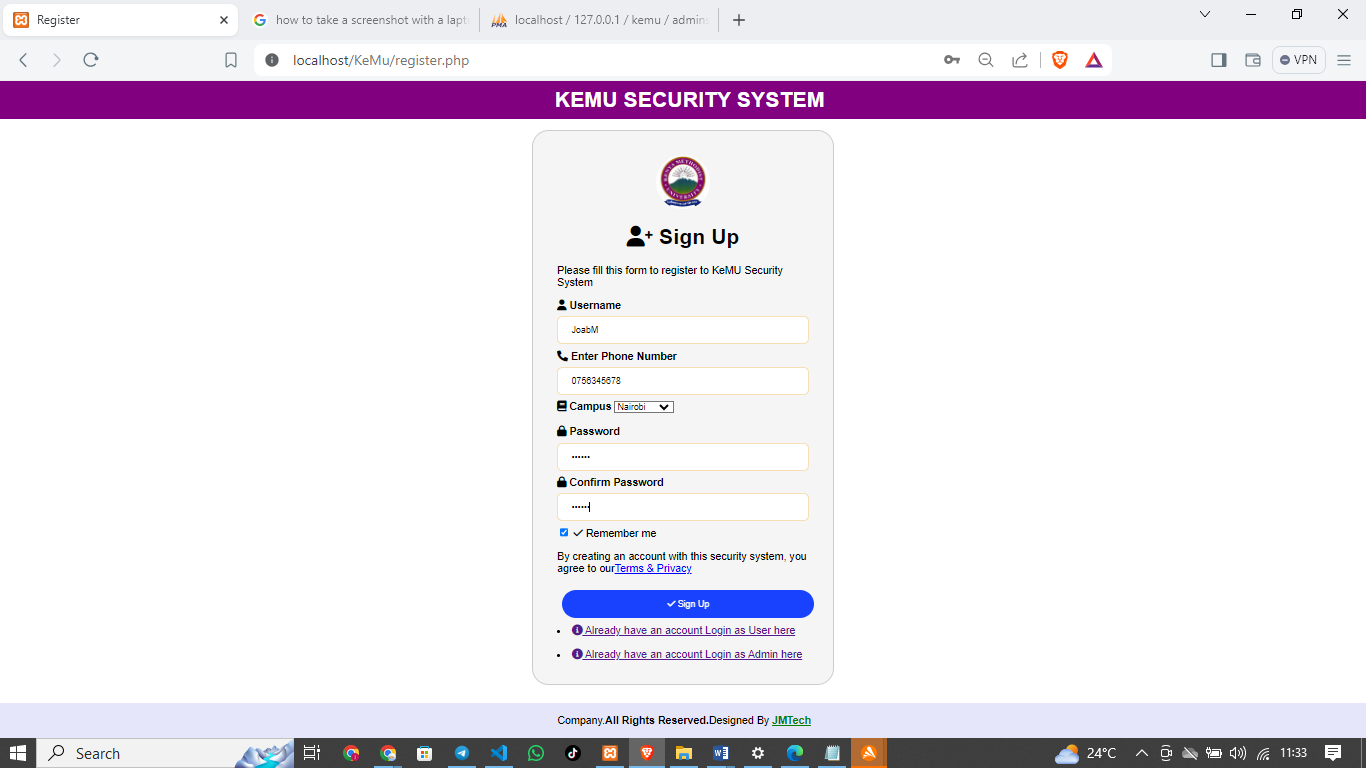
Sample Code for the hosts interphases



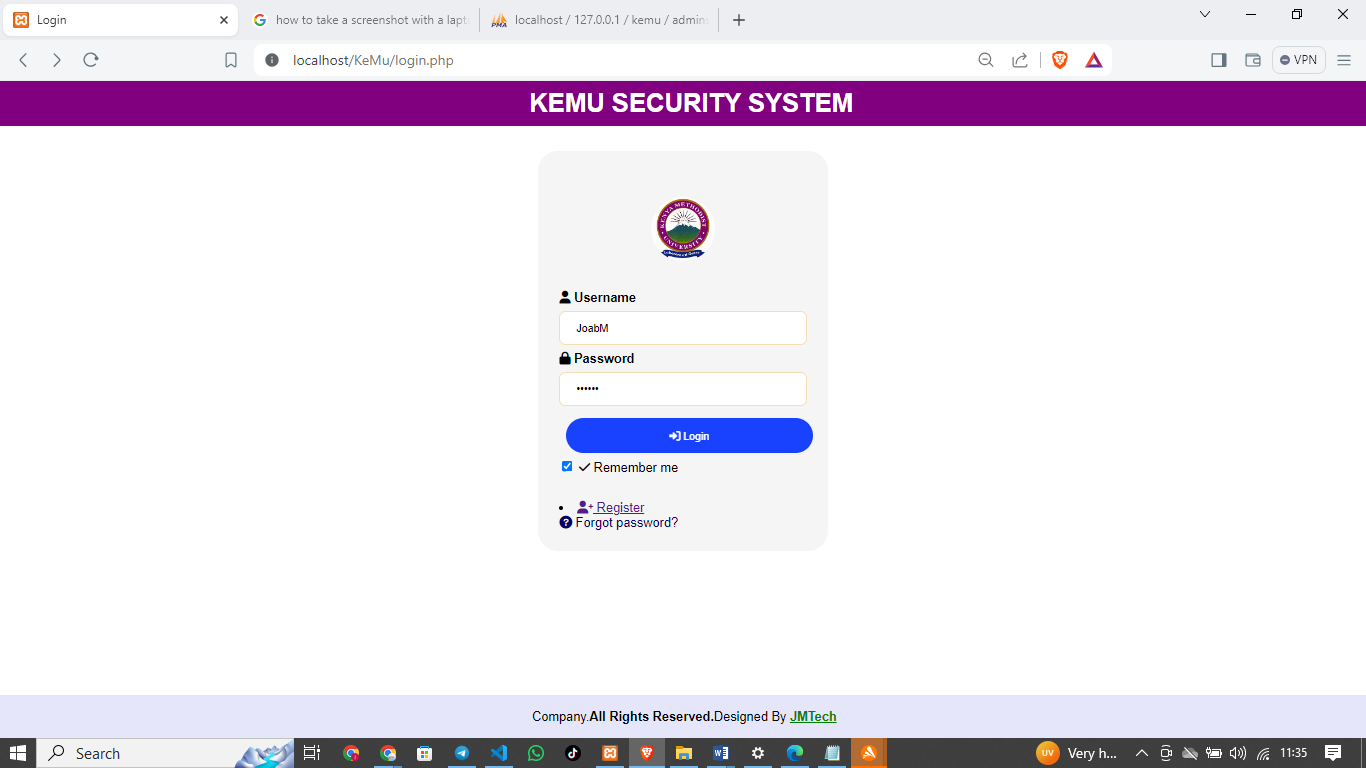
#### **5.2.1.3 User Sign-Up Functionality**

The system should include a sign-up functionality for new users, allowing them to create accounts by providing necessary information and verifying their identity.

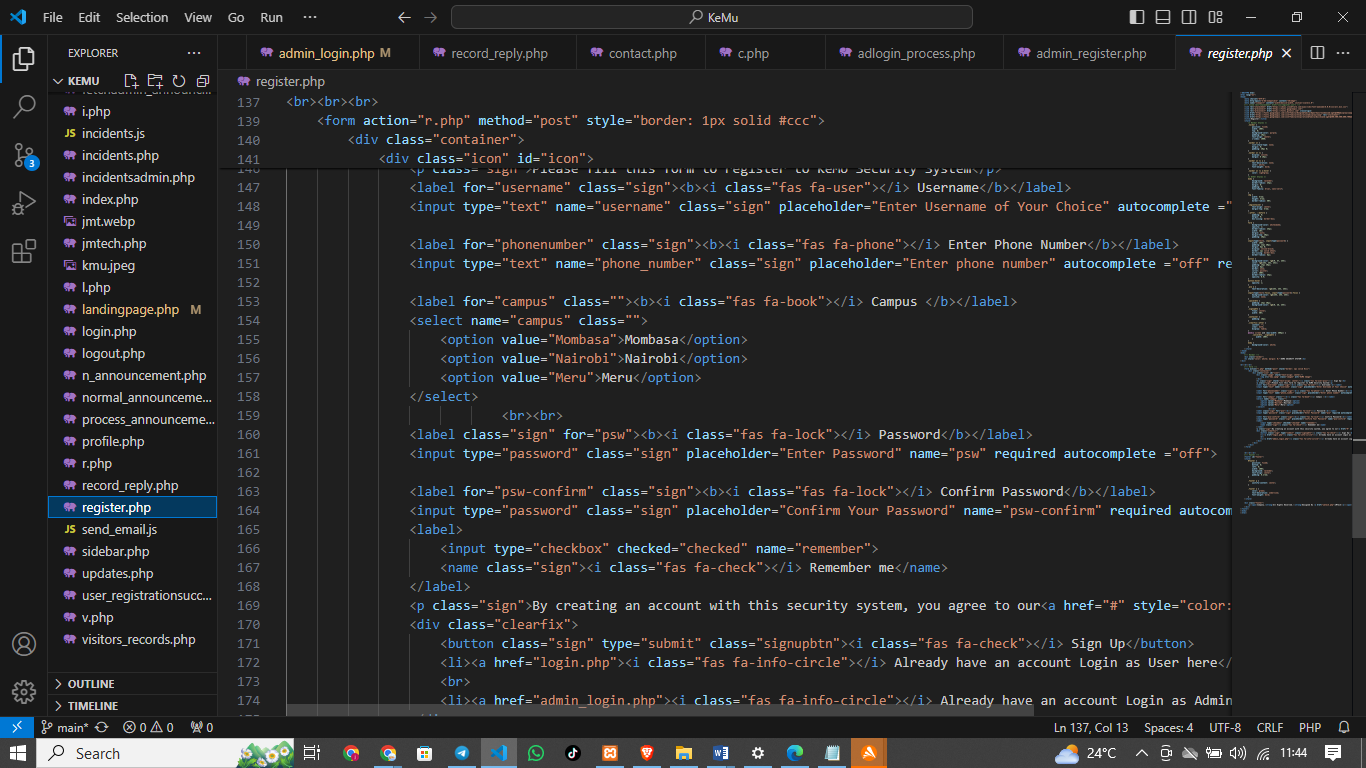
User Register Form



User Login Form



Sample codes



### **5.2.2 Communication Channel Between Senior and Junior Guards**

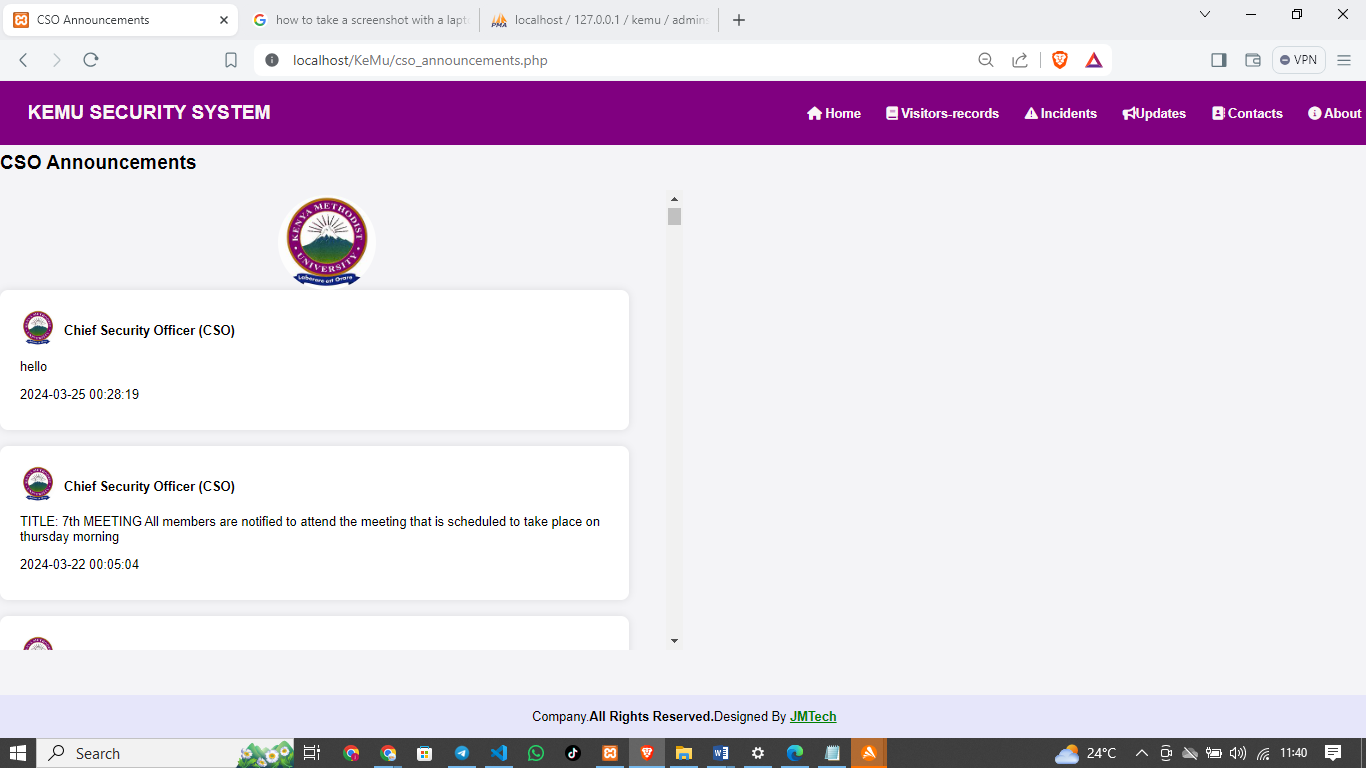
The Communication Channel Between Senior and Junior Guards is designed to facilitate efficient and seamless communication, ensuring swift response and improved coordination during security incidents.

#### **5.2.2.1 Messaging Interface**

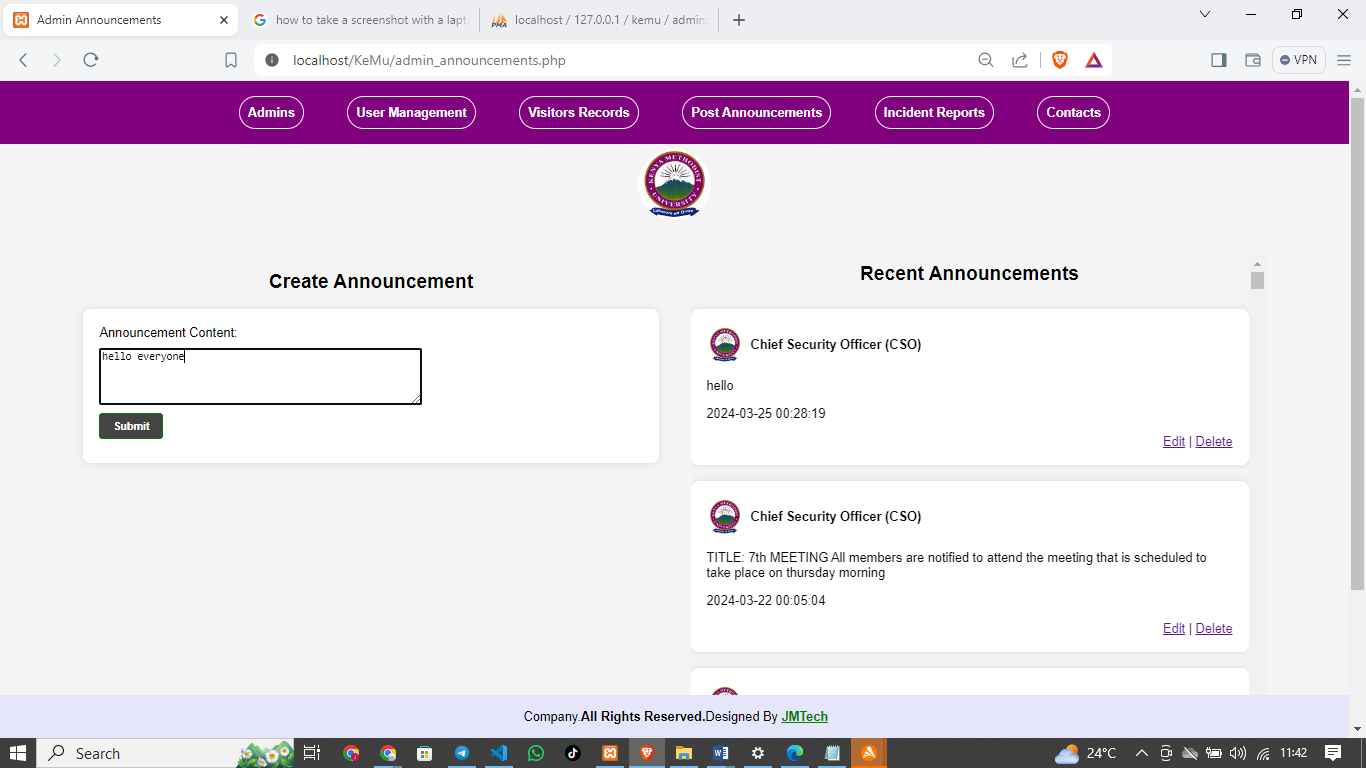
A dedicated messaging interface is needed for communication between senior and junior security guards. This interface should allow message composition, sending, receiving, and organizing messages based on priority or categories.

Communication Interfaces

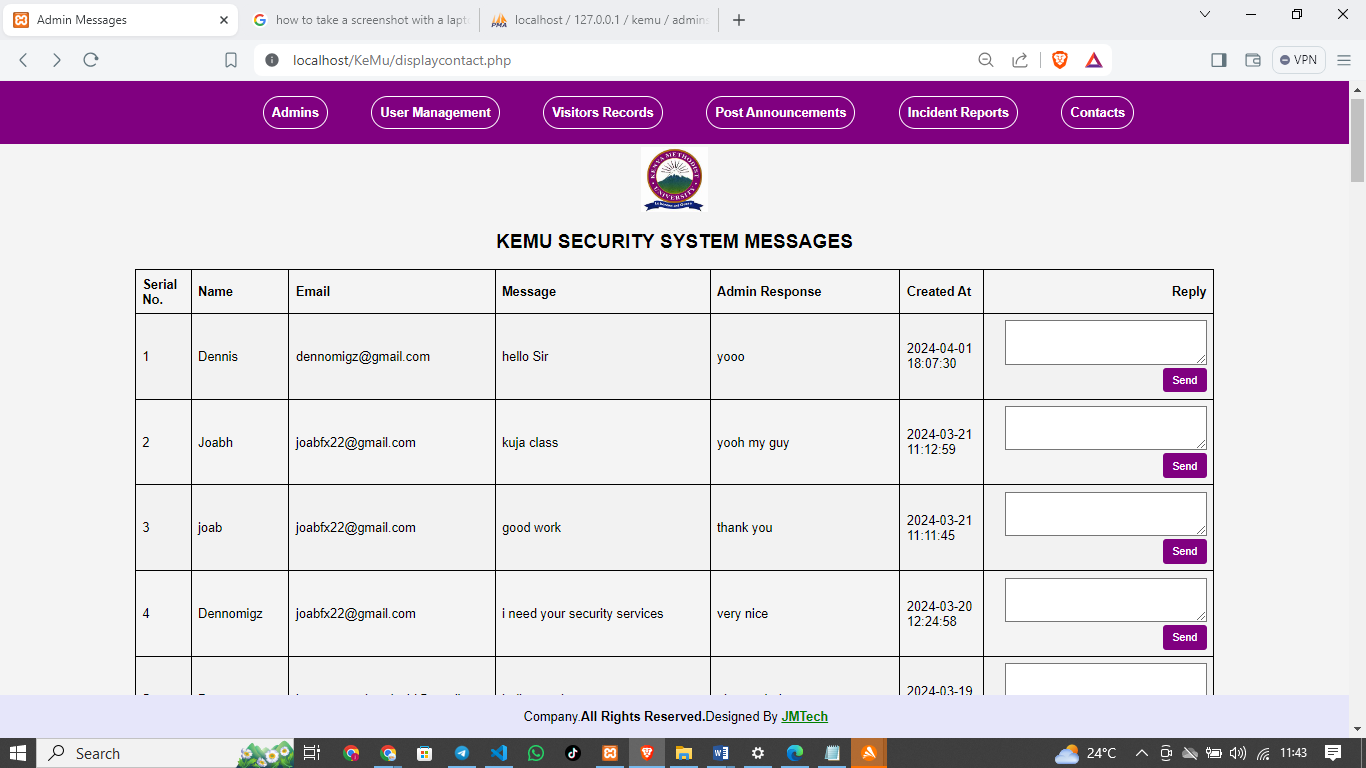
CSO announcements form



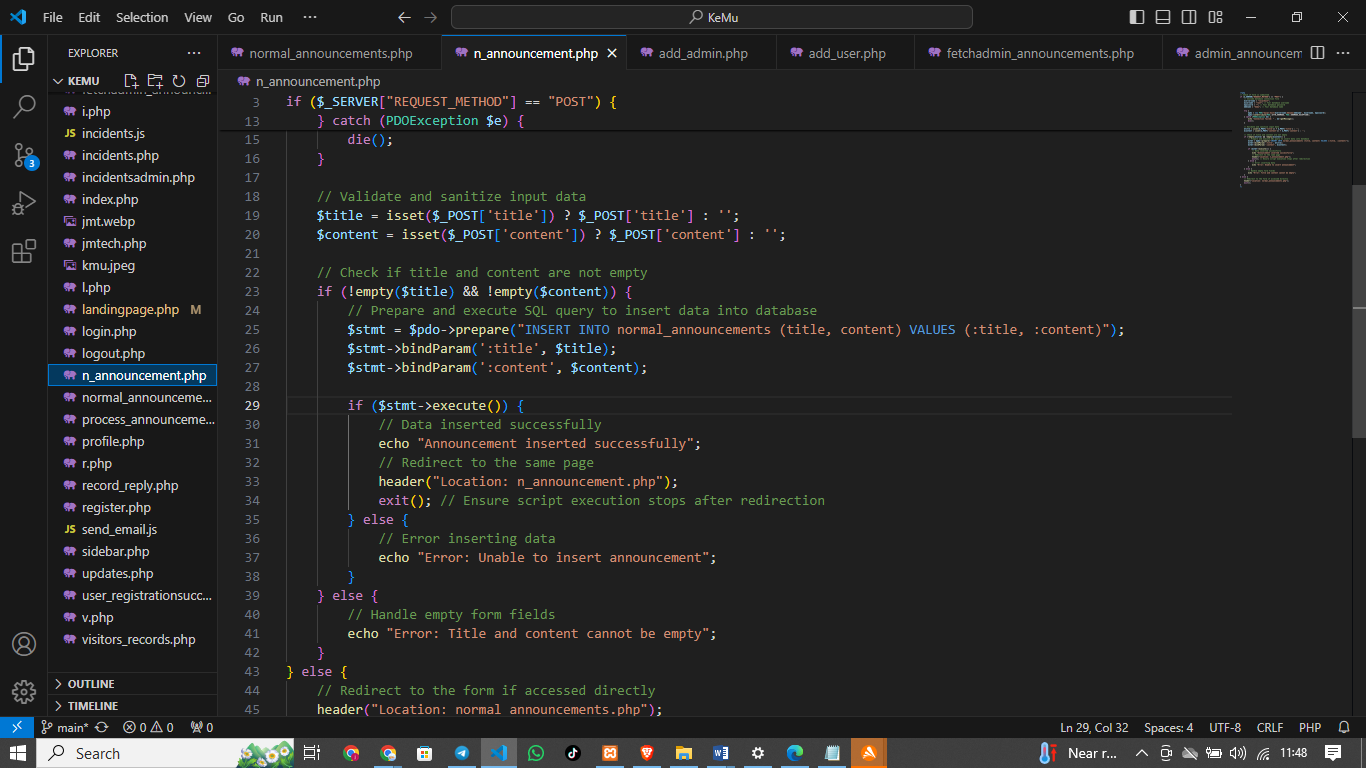
Admin announcements



Display messages section



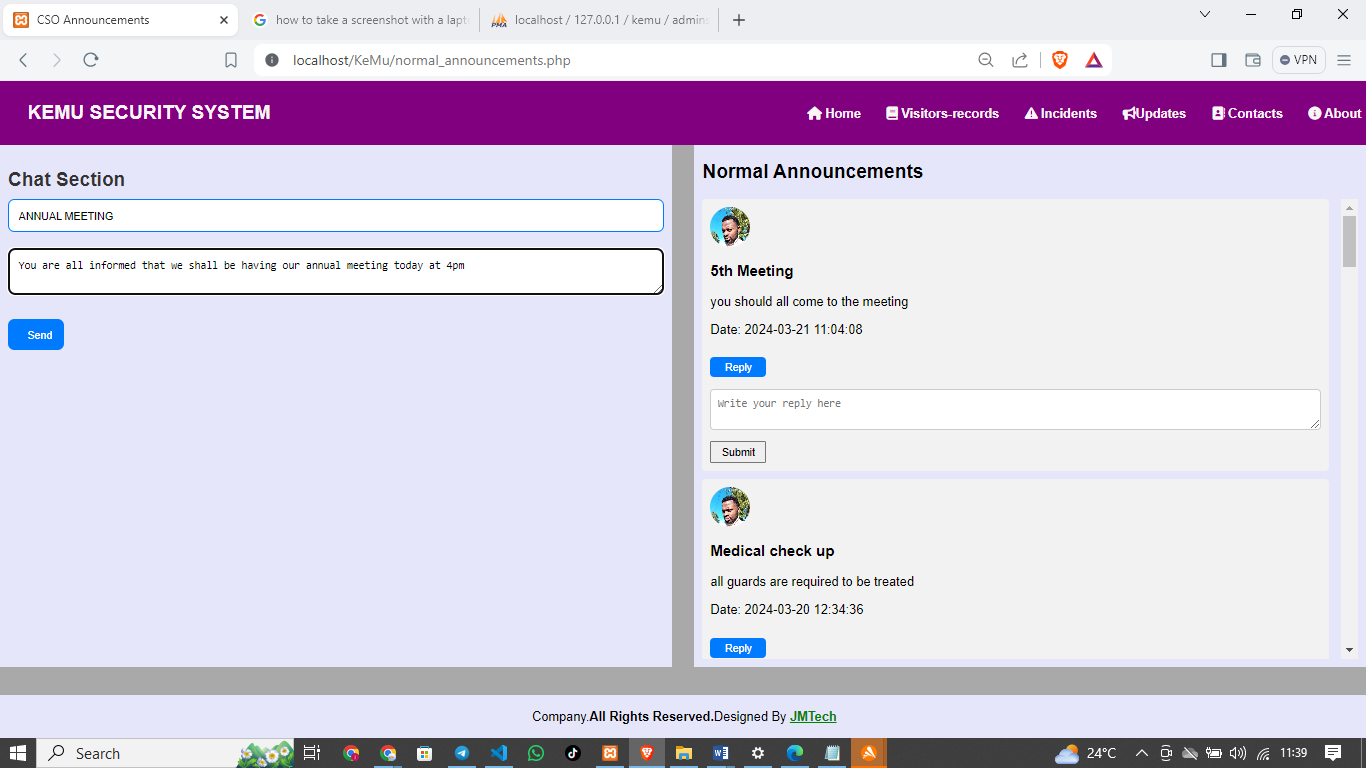
Sample codes



#### **5.2.2.2 Training Module Interface**

The system should include a training module interface accessible to security staff. This module will provide training materials, tutorials, and simulations for using communication tools effectively and following communication protocols during various security situations.

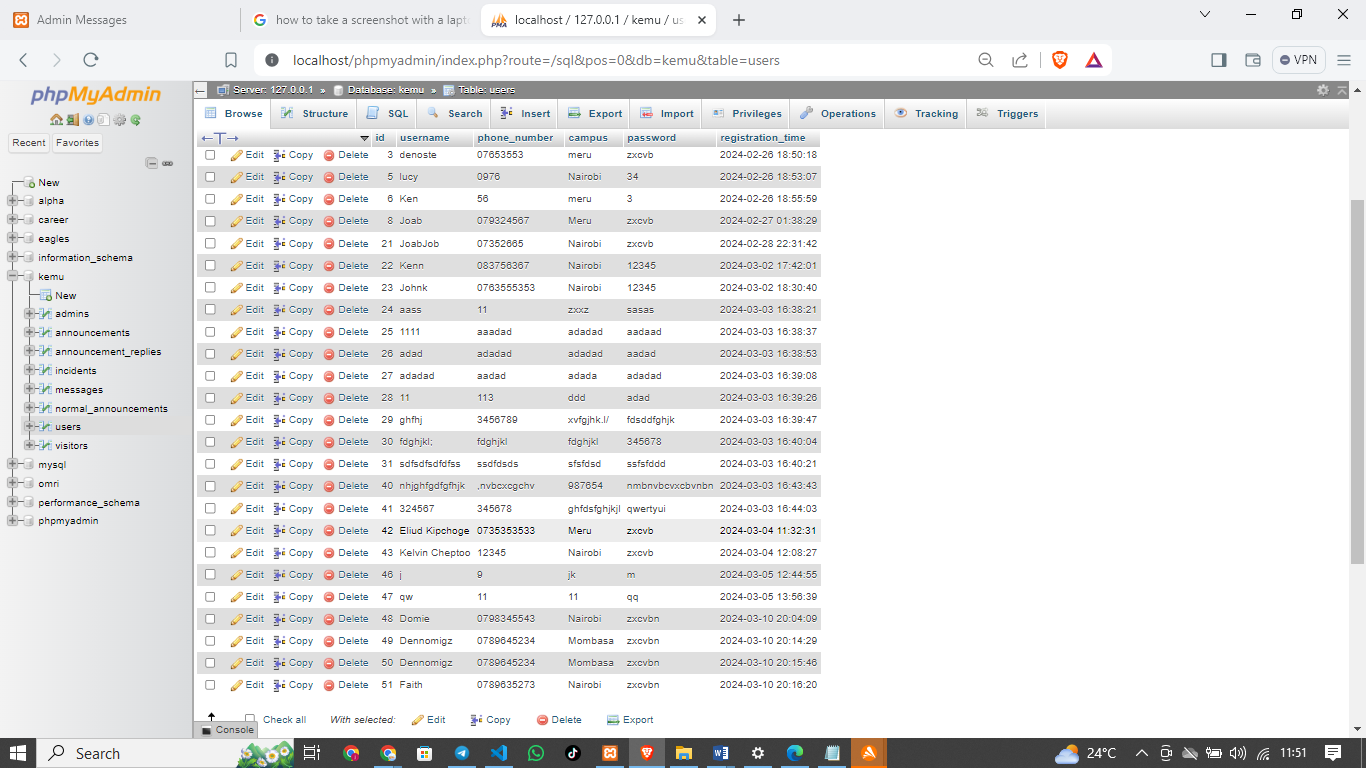
Training Interface



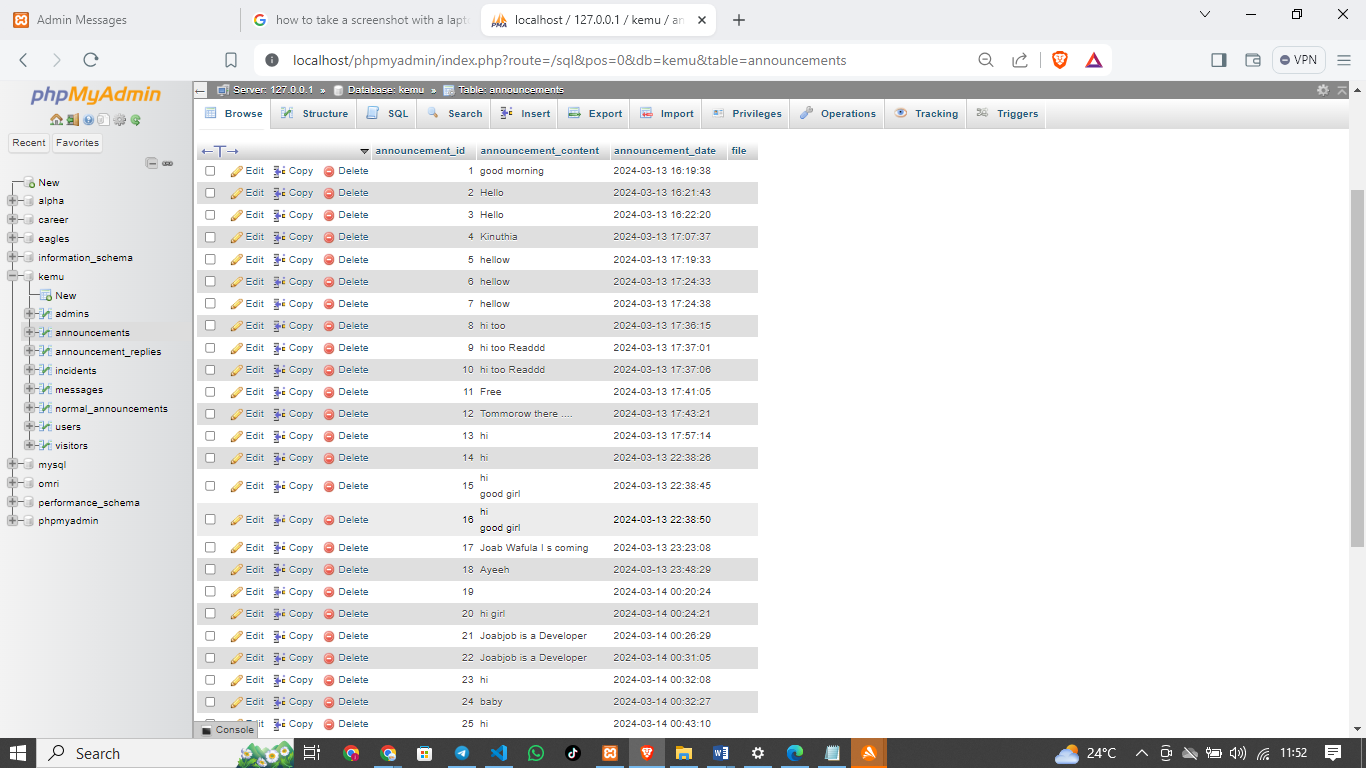
#### **5.2.2.3 Centralized Monitoring Interface**

An interface for centralized monitoring of security operations is essential. This interface will enable administrators to oversee communication channels, monitor messages, and ensure that responses to incidents are swift and well-coordinated.

Users in the database



Announcements recorded in the database



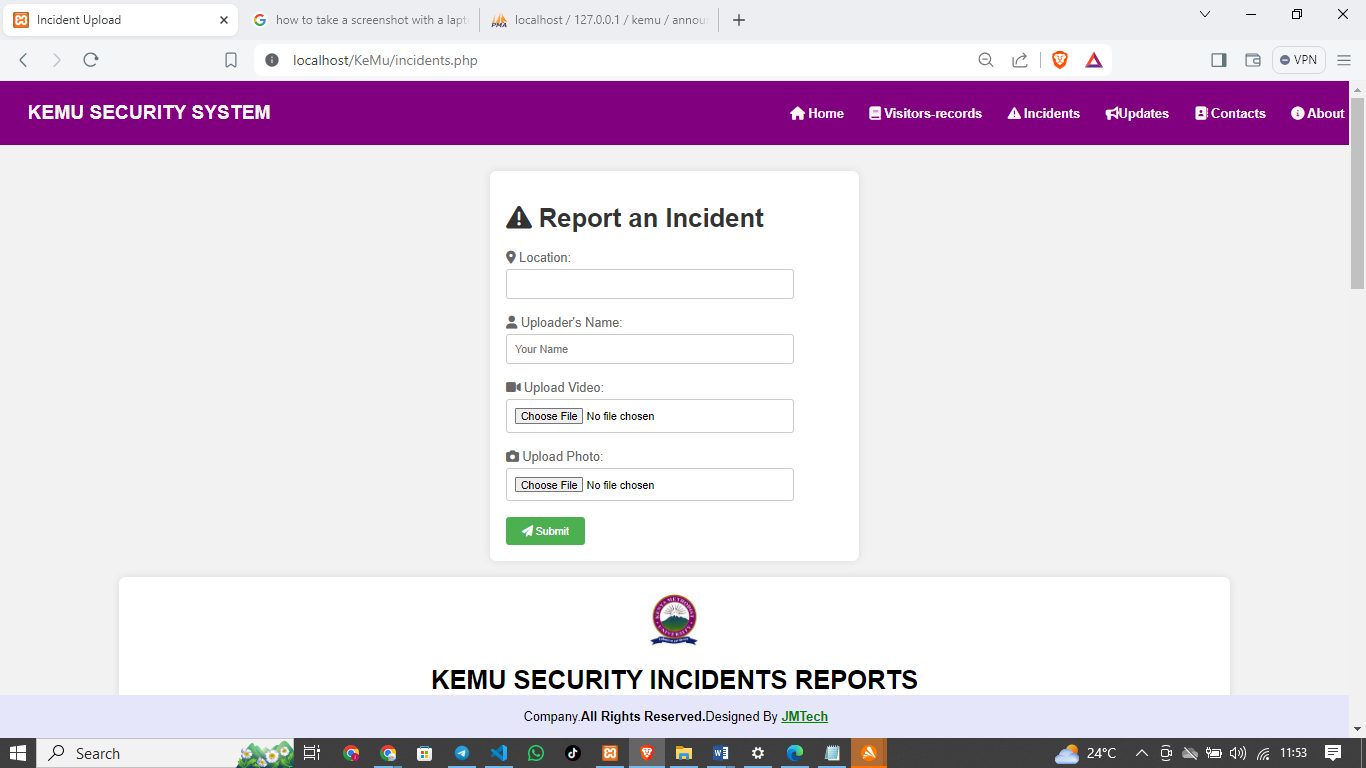
#### **5.2.3 Real-Time Recording of Incidents**

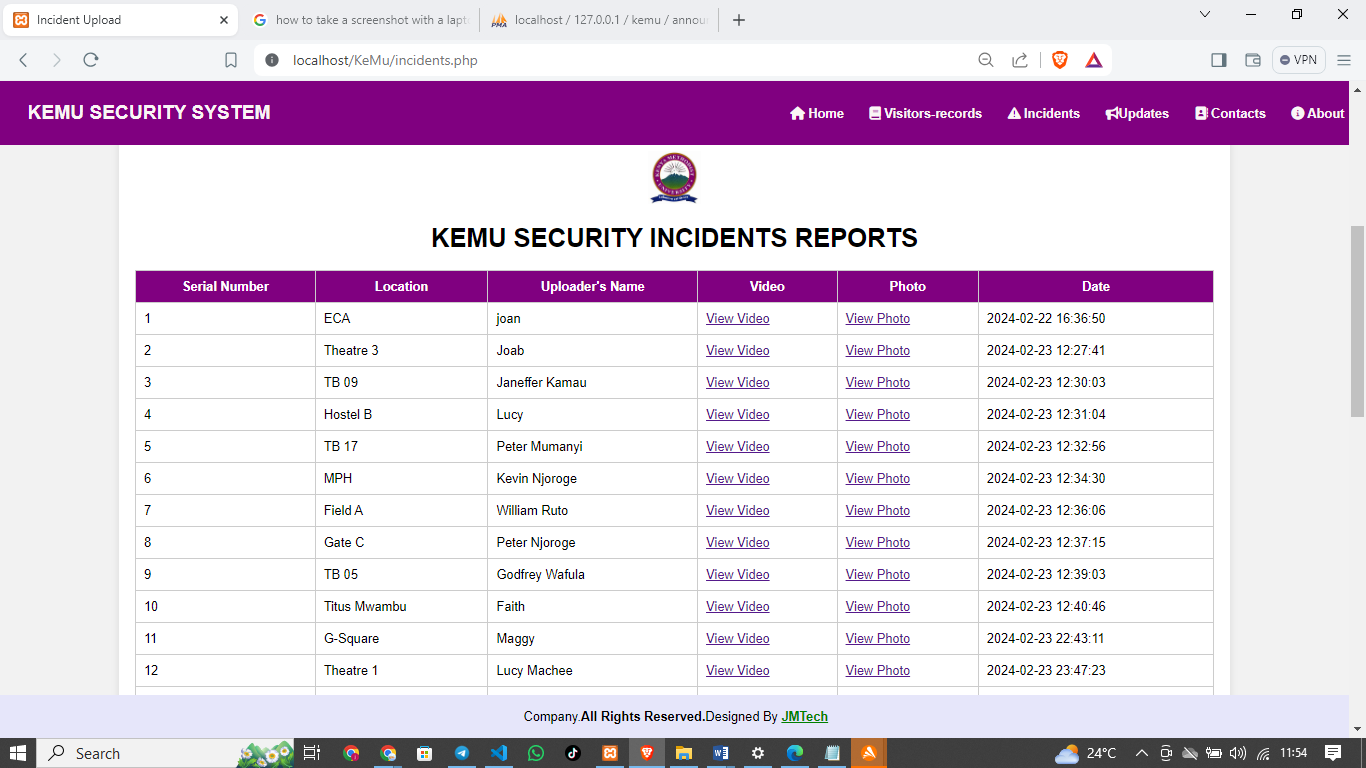
The Real-Time Recording of Incidents module enables the system to capture security events as they occur, providing accurate data for analysis and decision-making in ensuring a secure environment.

#### **5.2.3.1 Incident Reporting Interface**

The system must have an interface for incident reporting with fields for capturing incident details such as location, time, and nature of the incident. Security personnel should be able to log incidents in real-time using this interface.

Incidents records section

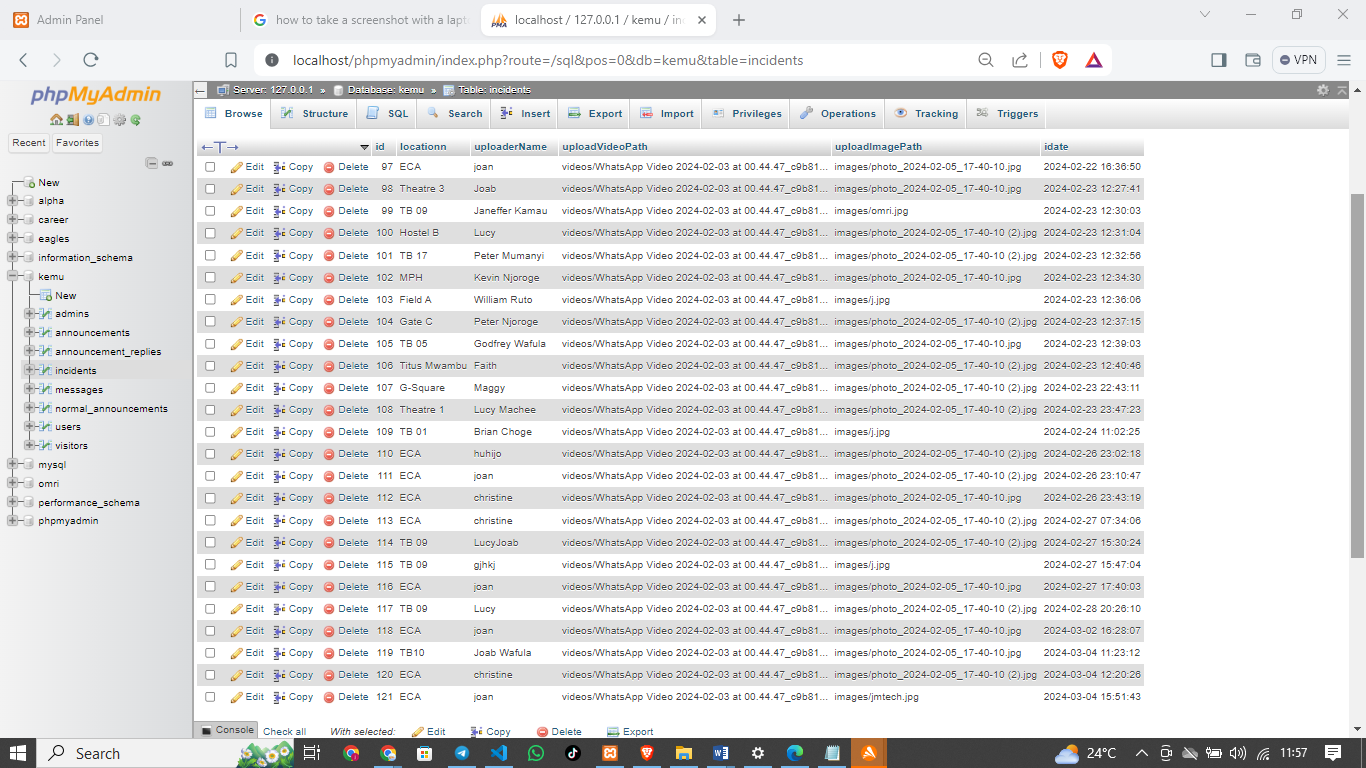




#### **5.2.3.2 Real-Time Recording Interface**

An interface for real-time recording of incidents is crucial. This interface will allow security personnel to document incidents as they occur, ensuring accurate and timely recording of security events.

Database section for recording incidents



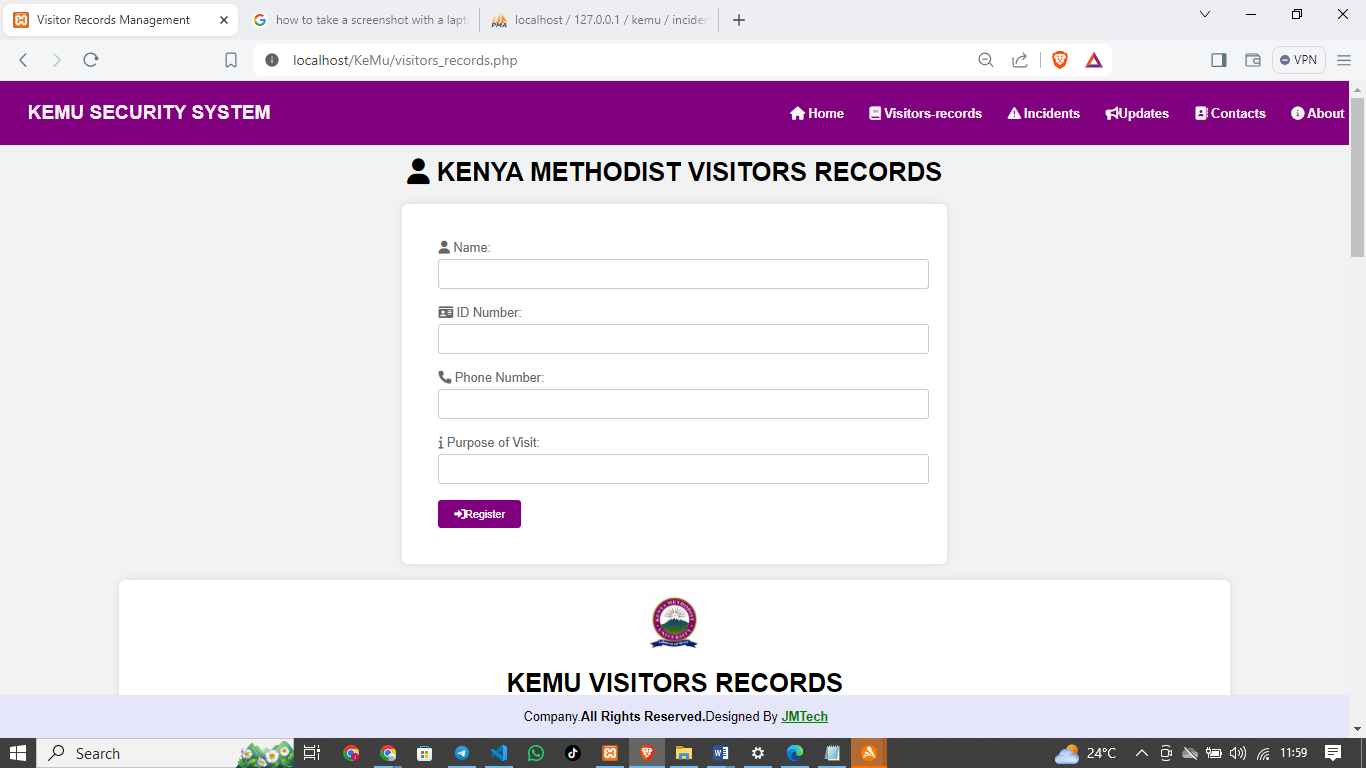
### **5.2.4 Visitor Records Management System**

The Visitor Records Management System module facilitates efficient management of visitor details, enhancing security and accountability within the campus environment.

#### **5.2.4.1 Visitor Registration Interface**

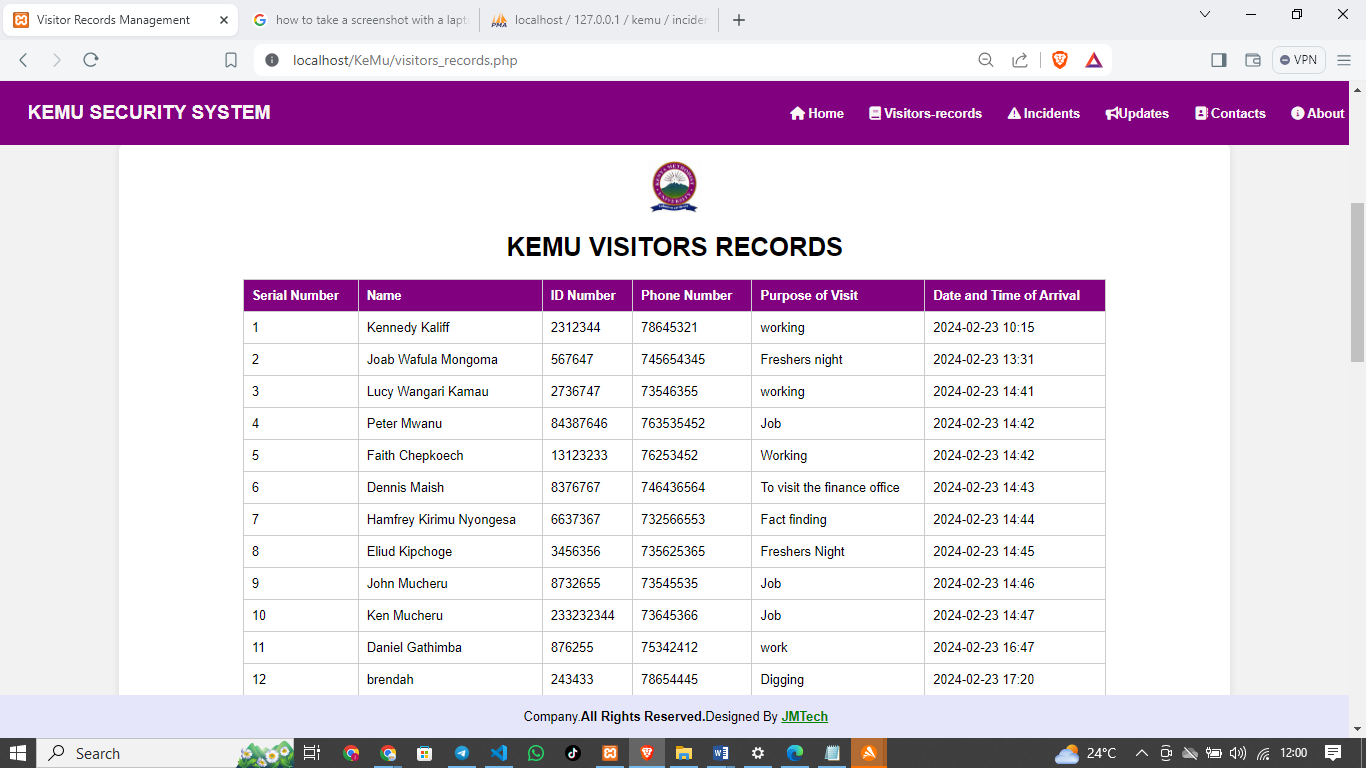
The system must have an interface for visitor registration, capturing visitor details such as name, ID number, purpose of visit, and vehicle registration number. This interface will allow for efficient visitor management within the campus.

Visitors Registration section



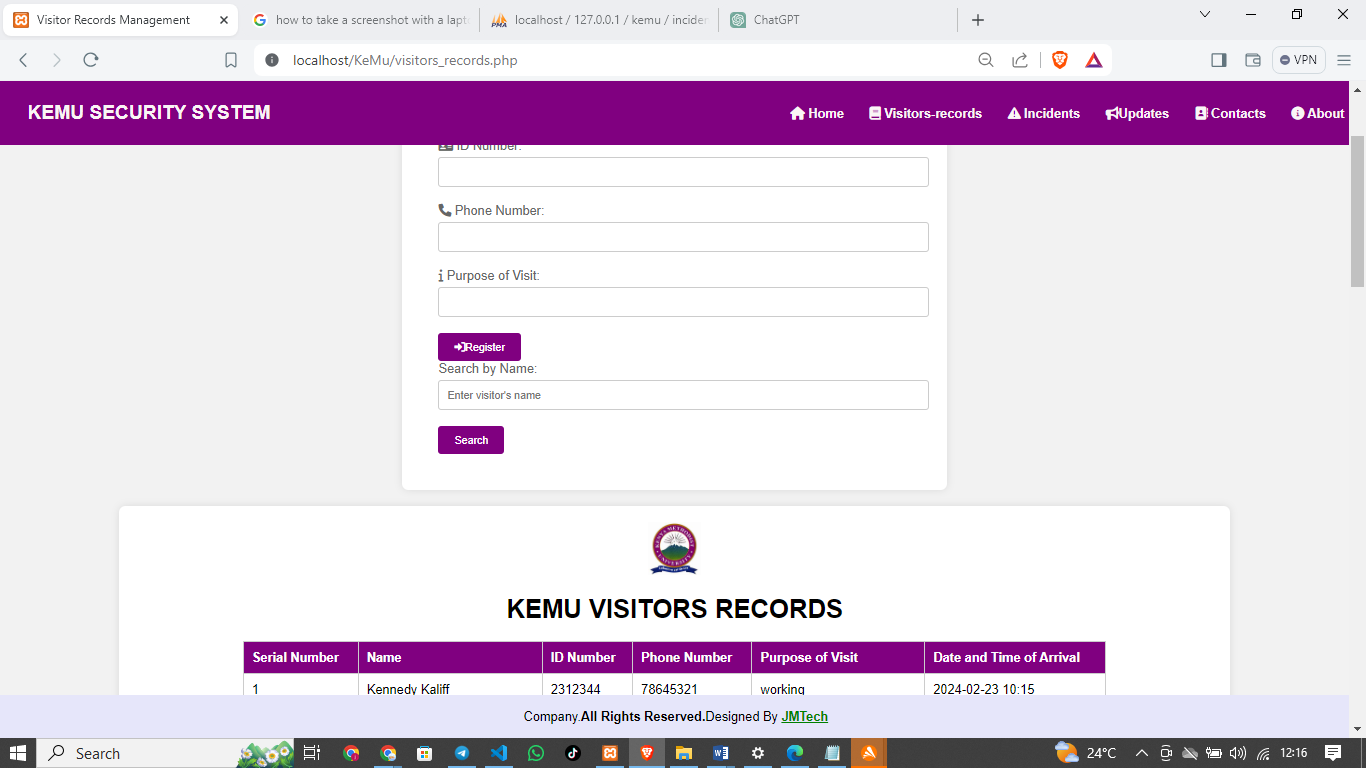
#### **5.2.4.2 Visitor Records Management Interface**

An interface for managing visitor records is essential. This interface will capture entry and exit times, track visitor movements, and provide search and filter functionalities for accessing visitor records.



#### **5.2.4.3 Search and Filter Interface**

The system should include a search and filter interface for accessing visitor records based on specific criteria. This interface will enable administrators to retrieve visitor information quickly and efficiently.



The detailed interfaces align with the functional requirements of the implemented security system, ensuring effective and efficient achievement of each specific objective. Integrating screenshots of these modules will visually demonstrate how the system meets each objective.

To integrate the specified security requirements into my project, distinct user roles will be established: Data Entry, Managers, and Administrators. Each role will have specific permissions tailored to their responsibilities. For instance, Data Entry users will enter requests but lack approval or deletion authority. Managers can enter and approve requests but cannot delete them. Administrators will have the ability to delete requests while being unable to enter or approve new ones.

Implementation-wise, the user interface of my system will reflect these roles and permissions. Users will only see functionalities relevant to their roles, ensuring a streamlined and secure workflow. Furthermore, a permissions management system accessible to administrators will be developed for assigning roles and configuring permissions as needed. The interface will provide clear feedback to users about their capabilities, promoting transparency and accountability across user categories.

## **5.3 Non-Functional Requirements of the Proposed System**

The implemented security system encompasses a range of non-functional requirements crucial to its performance and usability. Firstly, performance considerations are paramount, including factors like response time, throughput, and system utilization. The system must efficiently process user requests, handle data transactions promptly, and manage resources effectively to ensure optimal performance under varying workloads. Additionally, security requirements are fundamental, requiring robust data encryption, stringent access controls, and compliance with regulatory standards. Safeguarding data integrity, confidentiality, and availability is imperative, along with implementing robust authentication and authorization mechanisms.

Secondly, scalability and reliability are essential non-functional requirements for the implemented system. It should scale seamlessly to accommodate growing user bases and data volumes without compromising performance. Moreover, reliability measures such as fault tolerance and recovery procedures are vital to minimize downtime and ensure consistent system operation. Usability aspects also play a crucial role, demanding intuitive interfaces, accessible design, and user-friendly features to enhance user experience and productivity. Lastly, maintainability requirements focus on code readability, documentation quality, and support for future updates, ensuring the system remains adaptable and sustainable over time. These non-functional requirements collectively contribute to a secure, efficient, and user-centric security system.

## **5.4 Logical design of proposed system**

The logical design of the implemented security system involves creating an abstract representation of the data flow, inputs, outputs, and procedures to meet user requirements effectively. This design phase focuses on specifying user needs in detail to determine information flow, data sources, and system functionalities. Key components of the logical design include data flow diagrams and entity-relationship (E-R) diagrams to model data interactions and relationships within the system.

In the data flow diagrams, inputs (sources), outputs (destinations), databases (data stores), and procedures (data flows) are depicted to illustrate how data moves through the system and how processes are interconnected. E-R diagrams are utilized to define entities, their attributes, and the relationships between entities, providing a structured view of the system's data model. Together, these models form the foundation of the logical design, ensuring that the implemented security system aligns with user requirements and facilitates efficient data management and processing.

The figure below shows the logical design of the implemented security system.

Approve guards requests to use the system

Add/remove hosts(admins)

Post announcement

Add/remove guards

Guards

Record visitors

Record incidents

Communicate to the CSO

View announcements from the CSO

CSO

Registered?

Register

Login

Homepage

No

Yes

## **5.5 Physical Design of the Implemented System**

The physical design of the proposed security system revolves around ensuring efficient input and output processes, robust database design, and comprehensive backup procedures. This involves defining how users interact with the system, ensuring data accuracy during input, and presenting meaningful outputs. It also includes organizing data structures, establishing relationships, and implementing access controls in the database to maintain data integrity and security.

Additionally, specifying backup procedures is crucial for data protection and business continuity. This entails planning backup schedules, selecting appropriate technologies, and outlining recovery processes to minimize the risk of data loss and ensure system availability in case of unforeseen events. These procedures are essential components of the system's resilience and reliability.

Moreover, the physical design phase encompasses detailed planning for system implementation, including devising test and implementation plans, updating costs and benefits, setting conversion dates, and addressing system constraints. This comprehensive approach ensures that the security system is deployed effectively, tested thoroughly, and meets the defined objectives within specified timelines and resource constraints.

# CHAPTER SIX

# SYSTEM IMPLEMENTATION

## **6.0 Overview**

The implementation phase of the Kenya Methodist Security System marks the transition from development to deployment. This chapter outlines the testing, changeover/installation, and documentation processes involved in bringing the system to operational status.

## **6.1 System Testing**

### **6.1.1 Integration Testing**

Integration testing ensures that individual components of the system work together seamlessly as a whole. It verifies the interactions between modules and subsystems to identify and resolve any integration issues.

### **6.1.2 Unit Testing**

Unit testing focuses on testing individual units or components of the system in isolation. It verifies the functionality and behaviours of each unit to ensure that it meets specified requirements and functions correctly.

## **6.2 System Changeover/Installation**

**6.2.1 Parallel Changeover**

Parallel changeover involves running both the existing security system and the new system simultaneously for a period. This allows for a smooth transition as users can revert to the old system if issues arise with the new one.

**6.2.2 Direct Changeover**

Direct changeover, also known as "big bang" changeover, involves discontinuing the old system and immediately switching to the new system. It requires thorough preparation and poses a higher risk of disruption due to the sudden transition.

### **6.2.3 Phased Changeover**

Phased changeover involves implementing the new system gradually across different phases or modules. It allows for a more controlled transition, minimizing the risk of disruption to operations.

### **6.2.4 Pilot Changeover**

Pilot changeover involves implementing the new system on a small scale or in a specific department or location before full-scale deployment. It serves as a test bed to assess system performance and user feedback before wider implementation.

## **6.3 Documentation**

### **6.3.1 Internal Documentation**

Internal documentation includes technical documents, such as design documents, code documentation, and test plans, which are used by developers and IT personnel to understand and maintain the system.

### **6.3.2 External Documentation**

External documentation includes user manuals, operation guides, and system documentation, which are provided to end-users to help them understand and use the system effectively.

### **6.3.3 User/Operation Manual**

The user/operation manual for the Kenya Methodist Security System provides comprehensive guidance on system usage, operation procedures, and troubleshooting steps. It includes detailed instructions and illustrations to assist users in navigating the system and performing their tasks efficiently.

# 

# CHAPTER SEVEN

# CONCLUSION AND RECOMMENDATION

## **7.0 Achievements**

The achievements in developing the security system for Kenya Methodist University are significant and represent a successful effort to improve campus safety. One major achievement is the implementation of modern surveillance, access control, incident reporting, and visitor management systems. These systems have collectively enhanced security measures across the campus, creating a safer environment for everyone.

Another achievement is the system's improved operational efficiency. By handling user requests efficiently, managing data transactions effectively, and optimizing resource use, the system has improved workflow management within the security infrastructure. This has resulted in quicker response times, streamlined operations, and better resource utilization for security purposes.

Additionally, the system's user-friendly interfaces, intuitive design, and streamlined workflows have greatly improved the overall user experience. Security personnel, administrators, and stakeholders can navigate the system easily, leading to increased productivity, reduced training time, and higher satisfaction with the security infrastructure.

Moreover, the system's compliance with regulatory standards and robust security measures ensures data integrity, confidentiality, and availability. Strong authentication and authorization mechanisms further enhance security, providing a secure platform for handling sensitive information and reducing potential security risks.

Furthermore, the system's scalability and reliability are notable achievements. It can adapt to growing user bases and data volumes without sacrificing performance. Reliability measures like fault tolerance and recovery procedures minimize downtime, ensuring consistent operation and contributing to a dependable security infrastructure.

Lastly, effective change management during the system transition showcases successful project management and implementation strategies. The transition was managed smoothly, minimizing disruptions and ensuring a seamless experience for users.

## **7.1 Challenges**

Developing the security system for Kenya Methodist University faced several challenges that needed careful handling and strategic solutions. One major hurdle was integrating various security components effectively. This included ensuring seamless communication between devices, databases, and user interfaces while maintaining data security. Overcoming this involved thorough testing and fine-tuning of integration to ensure smooth functionality.

Another challenge was preparing for future scalability to accommodate more users and data. This required designing the system with scalability in mind, implementing scalable databases, and optimizing performance. Strategies like load testing and capacity planning were used to handle increased workloads effectively.

Meeting regulatory compliance and data security standards was also tough. This involved implementing strict security protocols, access controls, and data encryption. It required detailed risk assessments, robust security measures, and continuous monitoring to adapt to evolving threats.

Managing the changeover process during system transition posed challenges in terms of user training and workflow adaptation. Effective change management strategies were crucial, including user education and phased implementation, to ensure a smooth transition to the new security system.

In summary, addressing these challenges demanded a collaborative approach, proactive problem-solving, and continuous improvement to deliver a secure, scalable, and compliant security system for Kenya Methodist University.

## **7.2 The Proposed System Limitations**

The security system developed for Kenya Methodist University has certain limitations that are important to recognize for future improvements.

One challenge was adapting to new technologies and processes during the initial implementation, which required training and support to manage disruptions effectively.

Integrating multiple security components into a cohesive system was complex, requiring careful planning and ongoing monitoring for compatibility issues.

Scalability concerns may arise over time, necessitating optimization or upgrades to maintain performance with growing demands.

Cybersecurity risks are ongoing, requiring regular assessments and proactive measures to address potential vulnerabilities.

Budget and resource constraints may impact the system's ability to implement advanced features or upgrades quickly, necessitating strategic prioritization.

Understanding and addressing these limitations will guide future efforts in enhancing the security system's effectiveness and resilience.

## **7.3 Recommendation**

Based on the experience gained from developing the security system for Kenya Methodist University, several recommendations can be made to further improve its functionality and effectiveness.

Firstly, ongoing training and education programs should be implemented to ensure that users are proficient in utilizing the system's features and functionalities. This will help maximize the system's potential and enhance overall security awareness among stakeholders.

Secondly, regular audits and assessments should be conducted to identify and mitigate potential security vulnerabilities. This includes reviewing access controls, encryption protocols, and system configurations to ensure compliance with best practices and regulatory standards.

Thirdly, incorporating advanced analytics and artificial intelligence capabilities can enhance the system's ability to detect and respond to security threats proactively. This includes implementing anomaly detection algorithms, predictive analytics, and automated response mechanisms to improve incident response times.

Additionally, considering the evolving nature of cybersecurity threats, regular updates and patches should be applied to the system to address known vulnerabilities and ensure that it remains resilient against emerging threats.

Furthermore, fostering collaboration with industry experts, security professionals, and regulatory bodies can provide valuable insights and guidance in strengthening the security system's capabilities and addressing complex security challenges effectively.

By implementing these recommendations, Kenya Methodist University can further enhance the security system's effectiveness, resilience, and ability to safeguard its campus community and assets.

## **7.4 Conclusion**

In conclusion, the development and implementation of the security system for Kenya Methodist University represent a significant step towards enhancing campus safety and security. The system's integration of modern surveillance, access control, incident reporting, and visitor management systems has contributed to a safer environment for students, faculty, and staff.

Despite some limitations and challenges encountered during the project, the achievements are substantial. The system's operational efficiency, user-friendly interfaces, compliance with regulatory standards, scalability, reliability, and effective change management strategies highlight its success.

Moving forward, continuous training, regular audits, advanced analytics integration, regular updates, and collaboration with industry experts are recommended to further enhance the system's functionality and resilience against evolving security threats.

Overall, the security system stands as a testament to successful project management, technological innovation, and a commitment to ensuring the safety and security of Kenya Methodist University's campus community.

# QUESTIONNAIRE ON KENYA METHODIST SECURITY SYSTEM TO BE ADMINISTERED TO USERS

### ASSURANCE: THE DATA ENTERED BELOW WILL ONLY BE USED FOR RESEARCH.

(Kindly tick one in each question)

1. Please tick your gender

Male [ ] Female [ ]

2. Which campus are you from?

1) Meru [ ]

2) Nairobi [ ]

3) Mombasa [ ]

5) Other (please specify) ………………

3. What is your age?

15-20 years [ ] 21-25 years [ ] 26-30 years [ ] 31-35 years [ ] 36-40 years [ ]

4. Rate the Security services in the University out of 10?

A. Excellent 7-10[ ]

B. Fair 4-6[ ]

C. Worst 0-3[ ]

5. What features would you like to see in this Kenya Methodist Security System?

A. Easy registration process [ ]

B. Personalized profile [ ]

C. Integration with social media platforms [ ]

D. Other (please specify )………………………………

6. How important is it to you for the implementation of this KeMU security System?

A. Very important [ ]

B. Somewhat important [ ]

C. Not important [ ]

7. How likely are you to recommend this security system to others?

A. Very likely [ ]

B. Somewhat likely [ ]

C. Not likely [ ]

8. What other suggestions do you have for improving the security system?

…………………………………………………………………………………………………………………………………………………………………………………............................................

………………………………………………………………………………………………………………………………………………………………………………………………………………

# REFERENCES

Brown, A. (2020). Campus Security: A Comprehensive Guide. Publisher.

Davis, R. (2021). Collaborative Security Practices in Higher Education. Journal of Campus Safety, 15(3), 45-58.

Johnson, M. (2017). Emergency Preparedness in Higher Education. Academic Safety Journal, 22(4), 112-130.

Johnson, M., & White, S. (2022). Advancements in University Security: A Review of Current Trends. Journal of Campus Security Technology, 8(2), 77-92.

Jones, B. (2019). Access Control Technologies in Educational Institutions. Security Management Review, 14(1), 32-45.

Smith, C. (2018). Video Surveillance in Campus Security. Journal of Higher Education Safety, 10(3), 89-104.

Author(s) Last Name, First Initial. (Year). Title of the Book. Publisher.

Smith, J. D. (2020). Security Systems: Design and Implementation. ABC Publishing.

Journal Articles:

Author(s) Last Name, First Initial. (Year). Title of the Article. Name of the Journal, Volume(Issue), Page Range.

Johnson, A. B. (2019). Enhancing Campus Security Systems. Journal of Security Management, 15(2), 45-60.

Websites:

Author(s) Last Name, First Initial. (Year, Month Day). Title of the Web Page. Website Name. URL

Doe, J. S. (2021, March 15). Best Practices in Security System Development. Security Today. <https://www.securitytoday.com/best-practices-security-system-development>

# APPENDICES

# FEASIBILITY REPORT

### TITLE: FEASIBILITY STUDY OF KEMU SECURITY SYSTEM;

This feasibility study is focused on the evaluation of kemu security system. The proposed system aims to provide a platform for managing all security activities, such as visitors’ records keeping, incidents recording, communication channel and eliminating paperworks. The purpose of this feasibility study is to evaluate the viability of kemu security system and determine whether it is feasible to proceed with its development.

### OBJECTIVES:

User registration, login and sign up into the system

Communication channel between senior and junior security officials

Real-time recording of incidents

Visitor records management

### METHODOLOGY:

To conduct this feasibility study, I used a combination of primary and secondary research methods. I conducted an interview with security officers in the institution and the CSO and managed to gather the feedback on their current security system and potential benefits of implementing this proposed security system in their institution. I also conducted an interview with security department software developers to assess the technical and operational feasibility of the proposed system.

### RESULTS:

Market demand: there is a strong demand for the proposed security system 75% of the interview respondents indicating that they would be interested in using such system.

Financial viability: the proposed system is financially viable with a projected return on investment of 0ver 20% in four years.

Technical and operational feasibility: the proposed system is technically and operational feasible, with available resources and adequate infrastructure to support the systems operations.

Risk and challenges: the main risks associated with the development of the new system are related too potential data security and privacy concerns, as well as a potential user resistance to adopting the new technology.

### DISCUSSION:

The results of the feasibility study suggest that the proposed KeMU security system is viable and has a potential for success. However, there are risks and challenges that need to be carefully considered, particularly related to data security and user adoption.

### CONCLUSION:

Based on the results of the feasibility study, I recommend moving forward with the development of the new security system. The system has a strong market demand and is financially viable and the risks associated with the development can be mitigated through careful planning and execution such as implementing the appropriate data security measures and providing user training and support.

# APPENDICES

## **User/Operation Manual for Kenya Methodist Security System**

Table of Contents

Introduction

System Overview

Getting Started

Logging In

User Dashboard

Access Control

Granting Access

Revoking Access

Incident Reporting

Reporting an Incident

Viewing Incident Reports

Settings

Profile Settings

Notification Preferences

Troubleshooting

Glossary

Contact Information

## **1. Introduction**

Welcome to the Kenya Methodist Security System User/Operation Manual. This manual provides detailed instructions on how to use the system effectively for managing access control and incident reporting.

## **2. System Overview**

The Kenya Methodist Security System is designed to streamline access control processes and facilitate efficient incident reporting within the Kenya Methodist University campus. It allows authorized users to grant access to specific areas, report security incidents, and manage user profiles.

## **3. Getting Started**

**Logging In**

To access the Kenya Methodist Security System, visit the login page and enter your credentials (username and password). Click the "Login" button to proceed to your dashboard.

**User Dashboard**

Upon logging in, you will be directed to your user dashboard, where you can access various features and functionalities of the system.

## **4. Access Control**

Granting Access

To grant access to a specific area, navigate to the Access Control section and select the desired location from the dropdown menu. Enter the required details, such as the user's name and ID, and click the "Grant Access" button to confirm.

Revoking Access

To revoke access, go to the Access Control section and locate the user whose access you want to revoke. Click the "Revoke Access" button next to their name to remove their access privileges.

## **5. Incident Reporting**

**Reporting an Incident**

To report a security incident, navigate to the Incident Reporting section and fill out the incident report form. Provide detailed information about the incident, including the location, description, and severity. Click the "Submit Report" button to submit the report.

**Viewing Incident Reports**

To view incident reports, go to the Incident Reporting section and select the desired date range. All incident reports within the selected timeframe will be displayed, along with relevant details such as the date, time, location, and description of each incident.

## **6. Settings**

**Profile Settings**

In the Settings section, you can update your profile information, including your name, contact details, and password. Click the "Save Changes" button to update your profile.

**Notification Preferences**

You can also customize your notification preferences to receive alerts for specific events, such as access requests, incident reports, or system updates. Select your desired notification settings and click "Save Preferences" to apply changes.

## **7. Troubleshooting**

If you encounter any issues or technical difficulties while using the Kenya Methodist Security System, please refer to the troubleshooting section of this manual for guidance. If the issue persists, contact the system administrator for assistance.

## **8. Glossary**

This section provides definitions of key terms and concepts used throughout the manual to help users better understand the system and its functionalities.

## **9. Contact Information**

For further assistance or inquiries regarding the Kenya Methodist Security System, please contact the system administrator at [insert contact information].

This concludes the User/Operation Manual for the Kenya Methodist Security System. If you have any questions or require additional assistance, please refer to the contact information provided above. Thank you for using our system!

# PROJECT TIMELINE:

### SYSTEM INTRODUCTION AND CREATION

**7 days**: Define the scope of the project, identify requirements and create a project plan. Here, the integrated online sports management system is introduced and creating of the system begins.

### DESIGN THE SYSTEM

**14 days**: Implementation phase (1-3 months): Develop and implement the system, test it, and train staff to use it.

### DEVELOPMENT AND IMPLEMENTATION

**21days**: where coding is done and interfaces of the system is created with development tools like hardware and software. The system is then implemented.

### TESTING, TRAINING AND FEEDBACK

**28 days**: The developed system is tested to ensure it meets requirements or objectives of the proposed system and feedback given is used to show the response. Training of the administrative staff of the sports department, coaches and players to get feedback and correction is made

### UPDATE AND MAINTENANCE

**7 days –on-going*:*** the system is updated after some time and modification is made to improve and make it better. Maintenance is an ongoing activity that is continuous and provides support for the users of the system through system support.

### BUDGET:

The budget for integrating kemu security system can vary significantly based on the scope and complexity of the project.

To create a budget for this project, detailed information about the specific requirements and costs associated with each of these phases of the project. It is also important to factor in contingency costs for unexpected issues that may arise during the project.

Software licensing fees- Ksh.2000

Hardware costs (e.g. servers, network equipment) - Ksh.15,000

Development costs (e.g. customizations, integrations with other systems) - Ksh.50, 000

Implementation costs (e.g. training, data migration)-Ksh.5,000

Ongoing maintenance and support costs-Ksh.60,000.

Concluding, integrating a security system is a complex undertaking that requires careful planning and management to ensure success. By creating a detailed project plan and budget, you can help ensure that the project is completed on time, within budget, and meets the needs of the security department.