UNIVERSITI POLY-TECH MALAYSIA

SECURE STUDENT DISCIPLINARY RECORD MANAGEMENT SYSTEM

PUTRA AFIQ NASHRIQ BIN ABDUL HADI

BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN CYBER SECURITY

UNIVERSITI POLY-TECH MALAYSIA
Faculty of Computing & Multimedia

SECURE STUDENT DISCIPLINARY RECORD MANAGEMENT SYSTEM

PUTRA AFIQ NASHRIQ BIN ABDUL HADI
AM2311015270

FYP4085

AUGUST 2025

Declaration of Originality

This project is all my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet, etc.) has been acknowledged within the main report to an item in the References or Bibliography lists.

I also agree that an electronic copy of this project may be stored and used for the purposes of plagiarism prevention and detection.

Copyright Acknowledgement

Signed: 

Date:18th November 2025

Office Stamp

Abstract

The project presents a proposal of a Secure Student Disciplinary Record Management System which is to be used by the Admin, Staff in the Student Affairs Division and the Students of the university. Different disciplinary records are currently handled manually or paper based or stored in unprotected spreadsheets which is inefficient, has human error and can lead to data breaches. The proposed web-based system will offer an effective and secure system of managing such records by allowing functions like secure login, role-based access control, two-factor authentication, case-tracking, automated report generation, and providing secure access by the students to their respective disciplinary records. The project will help to enhance operational efficiency, make access control appropriate, and adhere to the Malaysian Personal Data Protection Act (PDPA). By using agile development method, the system will be developed, tested, and evaluated with feedbacks of actual university staffs in order to make sure that it is a good solution to the problems identified and enhances the overall disciplinary process.

Table of Contents

List of Figures

List of Tables

Acknowledgements

First and the most important; Alhamdulillah, all the praises to Allah, the might, the patience, and the guidance used in the Final Year Project (FYP2) completion.

I would also like to express my utmost gratitude to my beloved supervisor, Puan Nor Hafiza Binti Abd Samad, who has boosted, supported me professionally, and been able to give constructive criticism during this project. Her encouragement and advice gave me the power to work on time and improve my performance.

A special mention to Puan Norfazlina Binti Johar, Final Year Project Coordinator who tirelessly worked and ensured that all the students including myself were informed and guided throughout the FYP2.

I would also like to acknowledge my family and my parents who have been able to support me and pray and encourage me throughout my studies. Their support and encouragement have been the source of my strength.

I am grateful to MARA because they have provided me with the opportunity and education which have enabled me to pursue further studies.

I also owe the assistance of the staff and client of the Student Affairs Division, particularly, the Tuan Haji Yahya Bin Musa, the Senior Manager of Student Affairs Division (HEP) of the Universiti Poly-Tech Malaysia that provided valuable suggestions and ideas when planning on this system.

I would further like to express my deep gratitude to my examiner, Puan Nuri Surina Binti Abdul Halim, who has provided me with great feedback, insightful comments and constructive evaluation in the assessment of this project. Her advice and remarks have assisted me in sharpening my work and putting it into a more academic rightful perspective.

And lastly, though not the least, I would also like to thank all my classmates and friends too who helped me directly or indirectly by giving information, technical assistance, and moral assistance when I needed it the most. Thank you all for being with me on this journey.

1 INTRODUCTION

1.1 Introduction

Administering student records and particularly, discipline records in this internet era needs more than a file drawer or an Excel spreadsheet on the network. Much of the higher education is now high-tech, but far too frequently, the technology that the universities use to handle disciplinary records of students is low-tech. That will be a problem as far as efficiency, transparency, and data security are concerned. Due to the sensitivity and criticality of such a matter in the university administration, the lack of a proper digital system risks the university with lost files, data invasion, and delays in handling cases.

To resolve this problem, this project proposes the establishment of a Secure Student Disciplinary Record Management System. It will be a web-based application which will be tailor made to the administrative staff such as Student Affairs Division and also offer secure access to students. It will include systemized workflow of managing the cases of misconduct, secured access via differentiated role-based access, case tracking functionality and auto-reporting. It is not merely aimed at digitalizing the current process, but improving its reliability, accountability, and security according to the institutional policy and national data protection laws such as the Personal Data Protection Act (PDPA).

1.2 Project Background

Being among the functions of a university to preserve discipline and maintain a secure campus, there must also be a system whereby student misconduct is safely and properly documented accurately. But most of the universities, including ours, still employ manual or half-digital means, for example, paper forms, printed letters, or shared files but not securely stored. These are fundamental but possess a number of disadvantages such as data loss, duplication, delayed case updating, and even leaking of students' confidential information.

With increasing privacy awareness tied with legislation such as the PDPA in Malaysia, institutions of learning cannot continue to use unsafe practices when saving and handling personal data. Apart from legal compliance, workers at universities require a user-friendly, safe, and convenient system to track disciplinary cases, particularly when handling repeated occurrences or when generating reports for internal review. Furthermore, students are increasingly expecting transparent and secure access to their own academic and disciplinary records. That is the source of this project, which presents an organized, secure web application to the daily realities of Student Affairs personnel and provides students with direct access to their own disciplinary information.

1.3 Problem Statement

1.3.1 Manual and Unsecured Recordkeeping

Currently, discipline records are kept in paper files or loose electronic papers on local hard disks. It is a laborious system by which papers are easily misplaced, tampered with, or left undone. It is particularly inconvenient when the same student appears on multiple incidents, and workers are required to cross-match broken records.

1.3.2 Lack of Access Control and Data Privacy

The disciplinary records usually include sensitive information about students particularly their names, offences and consequences. In the absence of authentication and access control, there is a threat of unauthorized access, either unintentional or intentional. These breach of privacy of students and legal requirement of the university to maintain data protection according to the PDPA.

1.3.3 Inefficient Case Tracking and Reporting

Since there is no central system, it is cumbersome to keep track of the status of the current cases or generate reports. Employees are forced to search paper records or disorganized computer files to access past offences or a list of case resolution to meetings and audits. This would not only interfere with the backroom activities but it would also have an effect on the uniformity and fairness of case handling.

1.4 Project Objectives

1.4.1 To design and develop a centralized and secure web-based disciplinary record system that enables efficient creation, updating, and management of student misconduct cases.

This objective aims at establishing one centralized system in which all disciplinary records are kept and handled safely. The system will be replacing manual and disjointed processes, which will result in the staff and administrators being able to efficiently create new cases, update current records, and have a complete history of misconduct amongst students. Centralization eliminates duplication, loss of data and enhances consistency whereas the secure web-based design implies that the records can only be accessed through authorized channels. This directly responds to the inefficiencies and risks that are detected in the existing manual record keeping process.

1.4.2 To implement a secure login and role-based access control system that ensures only authorized users can access and manage sensitive disciplinary data.

This requirement underlines the significance of having high authentication and authorization rules in order to preserve confidential student data. The password hashing and the two-factor authentication (2FA) will help to secure the login process and the role-based access control will make sure that the user will only do what should be done according to his/her position. As an example, Admins are able to handle all cases and user accounts, Staff are able to report and update cases but not delete them whereas the Student can only view his or her own records. This stepwise security model implements the principle of least privilege, data confidentiality, and adherence to the personal data protection act (PDPA) in Malaysia.

1.4.3 To provide tools for structured tracking and automated reporting to improve transparency and efficiency.

This goal is aimed at making sure that the disciplinary cases can be tracked and recorded in a by-the-book fashion. The system has facilitated systematic monitoring by allowing the system to update status on the cases and upload evidences, which aids the staff and the administrators to be accountable and to ensure that no case goes unrecorded. Automated reporting programs enable users to produce official PDF documents and format them fast and precisely without the need to spend a lot of time on manual labor and errors. These reports can be used to aid in the audit process, internal audit, and decision-making process and also students can have a clear access to their disciplinary files. The system has been efficient by eliminating the hassle of tracking and reporting of cases hence fostering fairness in disciplinary management.

1.5 Scope and Target User

1.5.1 Project Scope

The project will concentrate on the development and design of a web-based application that will enable university staff to handle disciplinary records, and also students have a secure access to their own records in terms of cases. This involves the development of fundamental modules, which include secure access, role-based user access, creation and monitoring of cases, generation of reports and an administrative dashboard to control the system.

1.5.2 Product Scope

The end result will be the secure web application that can be accessed only by authorized university faculty and students. It will store the records in a relational database e.g. MySQL in a secure way and implement security measures like hashing of passwords, input validation, and Two-Factor Authentication (2FA). The system will also accommodate three roles, namely the Admin, who will have full access to the entire system, the entire database of the system, have full access to all the users, configurations and access to all the aspects of the disciplinary cases such as adding disciplinary cases, viewing current records and making amendments and updates, limited to a particular limit, the Staff, who will have limited access to the system, and have access to adding the disciplinary cases, viewing current records and updating/amending the details on the cases but to a limited number, and the Students, which will be very limited and only be able to view their own disciplinary cases and download the automated reporting PDF.

1.5.3 Target User

The main system users will be the Admin, Staff members of UPTM Student Affairs Division, and UPTM Students themselves. The Admin, who used to be a senior employee such as Tuan Haji Yahya bin Musa (Student Affairs Division Senior Manager at UPTM) will have the overall responsibility over the entire system and its database, and will control all the functionalities and user privileges and will be the supervisor over all the disciplinary procedures. The day-to-day running will be done by the normal Staff at UPTM Student Affairs Division where they will record new cases, update case details and view the records with a strict limitation to avoid such acts as deleting cases. Finally, Students will have an opportunity to access and review personal disciplinary records, which will be secured to allow accessing and viewing only personal records.

1.6 Overview of This Report

Chapter 1: INTRODUCTION

In this chapter, an introduction is provided to the Secure Student Disciplinary Record Management System including the background, problem statement, project objectives, scope and target users. It provides a background by establishing the aim of the project and difficulties in managing disciplinary records safely and effectively.

Chapter 2: LITERATURE REVIEW

The chapter examines available systems, practice, and academic literature in the area of student record management and data security. It contrasts existing solutions and underlines the gaps, which explains the necessity of a secure, centralized system of disciplinary records, which conforms to PDPA.

Chapter 3: METHODOLOGY

The chapter explains the adoption of the Agile methodology in system development. It will describe stages of planning, design, development, testing, deployment, and review, to show how the iterative approach was used to manage the project execution.

Chapter 4: REQUIREMENTS

This chapter describes the non-functional and functional requirements of the system. It provides the method of collecting requirements, in terms of questionnaires, interviews and observations, to make sure that the system fulfils the real needs of the real people to whom the system is intended that is, Admin, Staff and Students.

Chapter 5: ANALYSIS

This chapter interprets the data gathered so as to determine the user needs and operational problems. It has an interview finding, questionnaire results, use case models, and flowcharts to show how the system is supposed to be used.

Chapter 6: DESIGN

In this chapter, one is introduced to the system design, such as user interface wireframes, database schema, ERD, DFD, and security structure. It details the structure of the system such that it can be easily used, efficient, and meet the requirements of data protection.

Chapter 7: IMPLEMENTATION

The chapter describes the process of development and implementation of the system. It talks about the tools, platforms, and programming languages employed, and describes how modules like authentication, case reporting and report generation were deployed.

Chapter 8: TESTING

This chapter explains the testing procedure, unit testing, integration testing, system testing as well as acceptance testing. It also posts the user response and questionnaire results to assess the functionality, usability and security of the system.

Chapter 9: PROJECT MANAGEMENT

The planning and management of the project are brought out in this chapter. It contains work breakdown structure, Gantt chart and risk management plan detailing how everything was planned to keep the project on schedule.

Chapter 10: CONCLUSION

In this chapter, the paper will summarize the overall success of the project, pondering on the objectives achieved, achievements and challenges encountered and lessons learnt. It also gives future recommendations on how it can be improved like portal integration, real-time notifications, and analytics.

2 LITERATURE REVIEW

2.1 Introduction

The chapter critically reviews the literature, systems and security practices that can be used during the development of a Secure Student Disciplinary Record Management System. This literature review is aimed at exploring the emerging technologies, identifying the challenges and best practices and validating the implementation methods of this project. It also reveals the significant threats such as SQL injection which is one of the gravest issues of web applications development especially in the systems that deal with sensitive information such as student records.

Instead of paraphrasing every source in sequence, the aim of this chapter is to relate conclusions made from the different systems and scholarly writing to the situation of the present project. In it, it indicates how the conclusions made guide the design decisions of the project.

It also identifies the gap in current practice, specifically for local universities that continue to use obsolete manual processes, and justifies the necessity for a secure, centralized, and multi-role solution that adheres to data protection legislation such as the Malaysian Personal Data Protection Act (PDPA).

2.2 Investigation

This chapter develops the basis of the discourse for the Secure Student Disciplinary Record Management System through an organized analysis of its primary function, principal users, operating environment, and system architecture. In addressing these issues, the chapter establishes the basis for design considerations upon institutional requirement, privacy law, and secure development principles. The subsections address various aspects of the system to provide a consistent and well-structured rationale for its operation.

2.2.1 Secure Student Record System Overview

A Secure Student Disciplinary Record Management System is a web-based site that has the intention of recording and monitoring student misbehaviours in a properly structured and safe system. The main goal of the system is to make sure that issues with dress code, display of the car stickers improperly or not at all, unacceptable hairstyles are registered in a consistent and responsible system. The system maintains records such as student information, description of case, evidence, decision reached and the status of the case. This type of data shall be kept with integrity and only provided to the respective officers in charge and to the concerned student to ensure that there is no misuse of the disciplinary measure.

Electronic conversion of the process eliminates the common issues that are present in paper records and documents such as lost documents, bad handwritings, and lack of uniformity between the units.

The worth of such system can be understood considering the increasing need of transparency, accountability and compliance in higher education. Absence of an appropriate platform makes universities to mismanage cases, ignore serial offenders or violate the student privacy acts. The Malaysian Personal Data Protection Act 2010 (PDPA) specifies that the institutions are supposed to safeguard the personal data by ensuring their safety, restricted access, and open processes of handling the data. Furthermore, Miskam et al. (2023) indicate that most of the Malaysian private universities still use data protection strategies with hybrid solutions in managing sensitive student data. Through the use of an electronic disciplinary system that has built-in access controls and auditing, institutions will be able to equate what is practiced with the legislation at the national level and will be able to streamline its operations.

The high density of the disciplinary data also allows monitoring the cases better and eventually regarding patterns. The patterns that can be tracked by the university administrators include serial violators, disciplinary violators of most violators, and units with high rate of violators. The information is used to support the decision making and policy formulation of the administration and the intervention of student behaviour. In the paper by A Rahman and Norazah (2024), the authors emphasise the importance of the systematic monitoring of cases and safe data use in student behavioural systems with unmonitored data potentially leading to bias or habitual procedural failure. This will make a secure disciplinary management system not only a database but an instrument of preventing and enforcing academic integrity, prevention, and policies of an institution.

2.2.2 User Interactions and Functionalities

The disciplinary management is organised in terms of the types of users that are assigned their roles and duties. These are the Admin who will be in charge of the entire system, Staff who will key in new cases and update them as the case is being investigated, and Students who will have access to their own particular case details. All these positions will be granted access to a customized interface that has permission controls to work. This design would make sure that a user only accesses information that is relevant to their work and chances of sensitive information being accessed and edited by unauthorized personnel are minimal. According to Azameti and Adjei (2013), access roles are not defined in all educational systems meaning that the system is likely to be vulnerable to data redundancy and unauthorized access, which can end up being channelled to corroding the integrity of the whole system.

The system has a secure login page, a dashboard with a list of recent cases, forms to create new cases, and search history logs, which are all functional. Tested records can be filtered according to student ID. Case status tracking (Open/Closed) to provide accountability and transparency in the management of disciplinary cases. The future improvement is proposed as the use of notifications to enhance workflow.

These personnel-based, functional capabilities ensure the ease of workflow and normalization of the workflow that enables the user to track the progress, eliminate redundancy, and implement uniform procedures. As pointed out by Breeding (2023), not only do digital workflows in academic systems help to decrease administrative load, but they also enhance better data utilisation and timely action.

To make the system more usable, the system interface will comply with accepted standards of accessibility and responsive design principles. This will make sure that the system works well in different devices out of office equipment, laptops and even tablets during meetings. Action menus, the use of colour to indicate the status of a case and the automatic filling of student profile fields will ensure that the entry of erroneous information is minimized and it becomes a less technical experience to all the concerned individuals, including those not technically oriented. It will be designed under the user experience guidelines which have been evolved to the case of government and education websites with postponement to functional and simplicity as opposed to superfluous visual images. To promote the adoption of the system and ensure its long-term effectiveness in governmental agencies, Karim et al. (2022) support the legitimacy that the ability to use intuitively and a minimalist interface design are the most important factors to consider.

2.2.3 Integration with University Disciplinary Operations

The system is configured to become part of the day to day activities of the university departments that handle student behaviour. It does not substitute the existing processes, but provides an addition and optimization of processes to ensure that an employee can safely and more effectively perform tasks. E.g. case documentation, written or typed in Word documents, may now be uploaded via structured forms with dropdowns and date pickers to minimize the possibility of error during entry. Cases that are filed may also be checked faster by the concerned authorities hence reducing the delay caused by manual follow up cases. According to Yakubu et al. (2024), the general time of decision and consistency of documentation is improved among the departments of universities in case of switching to a structured case tracking scheme compared to the use of manual tools.

The system is implemented technologically in the form of HTML, CSS and JavaScript in the front-end interface which makes it user friendly. The server side is created with the help of PHP which offers powerful server-side features and smooth integration with MySQL. MySQL is the relational database management system, which is a stable and has good performance and organized data handling that is very applicable in an academic setting. It is an effective technology stack that ensures safe data transfer, effective user authentication, and scalable system architecture according to the needs of the institution. The security practices are input validation, session timeout setup, and password hashing with Bcrypt, as recommended with OWASP guidelines on how to establish a safe web application development (OWASP, 2023). Marking the cases as Open or Closed, means that the accountability and transparency in discipline management are achieved. Enforcement of CSRF token is suggested as a future-enforcement.

The deployment and testing are initially performed in a local environment with the use of XAMPP which enables the evaluation of interface behaviour and system logic to be done safely before full release. The demonstration and evaluation of the current system is on local deployment. To improve institutional adoption in future, improved features like encryption of the SL certificate, auto-database backup, and connecting the system to university authentication systems (e.g., LDAP, Active Directory, etc.) are encouraged to build on resilience and security, as well as simplifying accessibility. According to Al-Rousan and Al-Malah (2021), the systems, which align with the current digital infrastructure and the institutional policy, are more likely to be successful in the long-term perspective within the educational environment.

2.3 Related Works

The section identifies three practical systems that are used in the real world to explain successful methods of handling student data. These systems encompass features, user interfaces as well as workflow structures that are applicable to the proposed disciplinary record management system. The mentioned platforms are Kintone, iSAMS, and Zunia. All these platforms have easy user interfaces, strong data management systems and overall functionality to enable the management of cases or student records.

2.3.1 Kintone

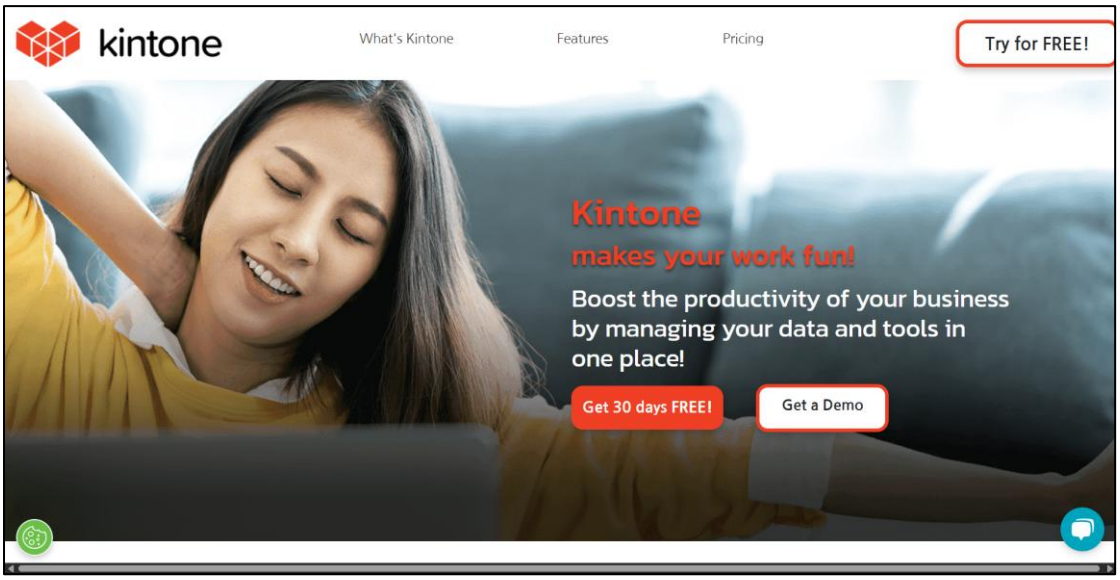


Figure 1: Kintone Home Page

Kintone is a management system for enterprises that institutions use to manage records, workflow, and tasks using customizable apps. It features a drag-and-drop interface that is easy to use for non-technical personnel to build and host forms for structured data. Kintone was not designed with education in mind but is used by most schools and universities to track student records, report incidents, and internal communications.

The application provides real-time collaboration, threaded discussion, file sharing, and permission management of users. It has an easy, elegant UI that promotes better delegation of task and responsibility, as one would want in a disciplinary system. Kintone's security system includes role-based privileges and access history log, thus confidential information is seen by intended users alone.

Yet the Kintone generic design has to be adapted to the tracking requirements of academic domains. While flexibility is an advantage, it may not have special education templates unless users create them manually. All the same, the system does show how cloud-based systems can be utilized in automating administrative functions securely.

2.3.2 iSAMS

Figure 2: iSAMS Home Page

iSAMS is an online school management software solution that many international schools and institutions use. It incorporates various behaviour monitoring and communication functionalities, attendance, record keeping, and interaction capabilities. The platform has a sleek and mobile responsive interface which can be accessed on desktop computers making it easy for teachers and admins to operate seamlessly.

The iSAMS system's behavior module permits staff members with the correct security clearances to capture behavioral incidents, assign actions, escalate matters, or tier cases transfer them to the relevant departments. In addition, it comes with analytic dashboards to monitor changes in students' behaviours over some time. School leaders or guardians of students can receive notifications and reports automatically generated by the system.

Business oriented solutions do not work together in the same workflows with the educational systems such as schools which makes iSAMS unique due to its applicability to education. In contrast to other systems where the student records are kept in different contexts of the policies of learning and teaching in a school - iSAMS supports all the workflows of the staff and entails automation, which allows integration with other school systems. This demonstrates that there is a need to have an efficient and secure inter-system collaboration when formerly closed systems need coordination with various departments, particularly in processes that may extend beyond the academic fields.

2.3.3 Zunia by Education Horizons

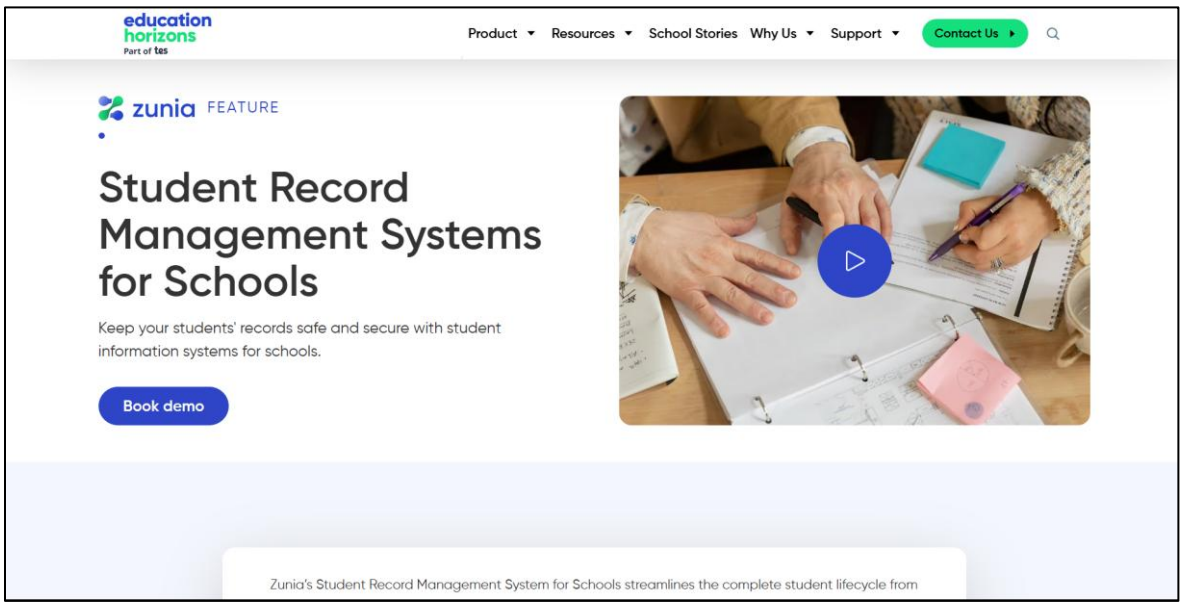


Figure 3: Zunia Home Page

Zunia is a student record management software that is specifically designed to manage the schools and is capable of managing the lifecycle of students, such as behaviour tracking, grades, health records and interaction history. Zunia has privacy and security features that are even more premiumized by putting an emphasis on ease of use.

The interface offers dashboards and data filtering and dynamic forms with its responsiveness and modernity. Its functionality of tracking of the incidents and their aftermath, tracing of their follow-up and the provision of the necessary support qualifies Zunia behaviour module as semi-automation in the framework of larger systems. In addition, Zunia can send alert messages to the staff and provide real-time updates to the families about the need to respond on time without lacking transparency.

One of the factors that Zunia stands out is that the steps of recording, reviewing student incidents, or correcting related cases are simplified in one workflow. Marking clear lines between complexity and usability would be one significant marker when creating a focused disciplinary case management system at the university level. It is also worthy to note that it complies with the data protection laws that strengthen system objectives to support your project rationales.

2.4 Comparison

The following table offers a comparison of the three systems, which were mentioned in the Section 2.3, which are Kintone, iSAMS, and Zunia. It pays attention to the essences of their functionality, the ease of use of their interface, security aspects, and their general appropriateness to handle disciplinary records in schools. This comparison assists in the determination of the strengths that would be adopted and weaknesses that could be overcome in the development of the proposed Secure Student Disciplinary Record Management System.

Criteria	Kintone	iSAMS	Zunia
Type of System	Business workflow management	School management system	Student record & behavior management
User Interface (UI)	Clean, flexible drag-and-drop app builder	Professional, mobile-friendly, school-branded	Modern, clean, highly accessible
Disciplinary Logging	Customizable via user-created forms	Built-in incident logging and behavior tracking	Behavior module with follow-up and alert functions
Search/Navigation	Real-time record search and filters	Searchable history and reporting tools	Searchable dashboards, filters for roles and events
Security Mechanisms	Role-based access, basic audit logs	Secure login, role-based permissions	Secure login, privacy-compliant, access controls
Customizability	Highly customizable, flexible modules	Limited to predefined academic workflows	Customizable templates and dashboards
Target Users	Businesses, adaptable to schools	Large and international schools	Schools and educational institutions
Advantages	Flexible, collaborative, easy to set up	Feature-rich and tailored for academics	Education-focused, streamlined for discipline
Disadvantages	Not education-specific; manual setup needed	Complex, may be expensive or require training	Subscription-based, limited free access

Table 1: Comparison of Existing Project

2.5 Discussion

It can be concluded that, according to the analysis and comparison of Kintone, iSAMS and Zunia, all the systems have valuable features that could help in shaping up the proposed Secure Student Disciplinary Record Management System. This part is an explanation of the most important lessons learned in those systems, and how their functions, security measures, and constraints can affect the design choices in the proposed project.

To begin with, Zunia is a very good example of a student discipline and behavioural data monitoring in a learning institution. Its capacity to record events, trace them and send automatic notifications will ensure that university staff take the necessary steps in time. Its filtered user interface and workflow-based education designate it as a wonderful contender of user experience and behaviour tracking. The suggested system will be an extension of the notification and incident report capabilities of Zunia so that student affairs personnel can manage the cases of misconduct more effectively. Secondly, its security access privileges and user accounts increase the significance of the protection of sensitive data about students. The same will be emulated in the proposed system through the use of differentiated role-based access control, as well as encrypted user login processes to all the types of users, including the students.

Secondly, iSAMS integrates a robust set of academic tools in a single school management platform. Its modular design for tracking and analyzing behavior allows schools to gain insights into patterns of misconduct and take prevention measures accordingly. These analytics would be especially valuable to deans or university disciplinary committees that need to analyze trends over a number of semesters. While the complexity of iSAMS may not be suitable for smaller institutions, the role-based dashboards and reporting capabilities idea will be achieved in a lessened and condensed way in the proposed system. This is accompanied by an examination of incident escalation and review workflows within iSAMS that the project will include similar review and approvable procedures tailored towards a university environment.

Lastly, while Kintone is not designed with education in mind, its biggest advantage is flexibility and low-code interface. This allows users to design their own record-keeping applications without much technical expertise. The suggested system will take the strengths of Kintone's form customization, modularity of field management, and data filtering. Contrary to Kintone, the proposed system will feature pre-defined disciplinary templates and institutionally based workflows. This eliminates the requirement to manually implement technical components. In addition, Kintone's threaded comment and co-editing note feature offers a good suggestion for integrating feedback logs on each case in the proposed system, which can promote communication and openness among employees.

2.6 Conclusion

This chapter has presented a comprehensive literature review and system discovery for the design of the Secure Student Disciplinary Record Management System. It initially defined what a disciplinary record system is, why it matters, and how universities can more effectively and securely manage instances of student misconduct using computerized procedures. During the investigation, it was found that manual record-keeping methods used in the majority of institutions not only become time-consuming but also pose security threats to data and are non-conformant to acts such as the Personal Data Protection Act (PDPA) of Malaysia.

Three systems used were examined to investigate current student data and behavior management methods: Kintone, iSAMS, and Zunia. Every system offered different strengths in terms of interface design, integration of feature set, and workflow management. Kintone identified flexible data management and user customization as strengths. iSAMS displayed organized educational workflows with behavior modules integrated. Zunia emphasized simplicity, ease of use, and education-oriented features. These rival works were contrasted and expounded upon to determine which elements could be adapted and improved upon in the system proposed.

In conclusion, this chapter provides the foundation for the following project phase: system design and development. The proposed Secure Student Disciplinary Record Management System will borrow top features such as incident logging, differentiate user role access, secure authentication, and reporting dashboards, from the systems under review. It appears to fill the current divide between too complicated enterprise systems and sub-elevated manual procedures, presenting a suitably balanced resolution aimed at addressing the specific needs of a Malaysian university setting, including secure and transparent access for students to their own disciplinary records. The discoveries made here ensure that the system will be developed with user satisfaction, compliance, and usability in mind.

3 METHODOLOGY

3.1 Introduction

In this chapter, the methodology and the techniques employed in coming up with the design of the Secure Student Disciplinary Record Management System are described. It includes project methodology, tool and technology to be used on the project, system design process, data collection methods and testing plan. The aim is to make sure that the system is designed in a methodical manner and is able to accommodate its functional, security and multi-user requirements.

3.2 Agile Methodology

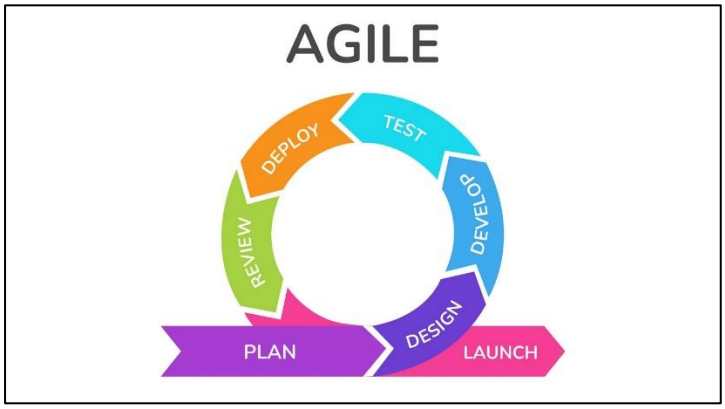


Figure 4: Agile Methodology Diagram

In the case of this project, the Agile Methodology has been selected. Agile is a cyclic and flexible approach that prefers continuous enhancement, fluidity to critical layout, and consistent feedback of the stakeholders. Such a system would best suit because it would be developed in stages, with each stage creating different modules of the system that include login security, track cases, reporting and differentiated access control, which would meet the specific requirements of the Admin, Staff, and Student users.

Agile technique will be adhered to with the use of short-term development cycles also known as sprints. A sprint will take two or three weeks and will provide a functional part of the system. This gives room to continuous testing and reworking until the final product is as desired by the users and is in accordance with the data handling policy of the university.

The iterative approach of Agile also gives the developer an opportunity to respond to the changes in project requirements or emergent issues in the implementation. It involves communicating with the supervisor, client, and other important stakeholders where the short feedbacks and continuous enhancement is realized throughout the life cycle of the system.

3.3 Phases in Agile Methodology

Agile Methodology has a flexible and iterative process. Agile method breaks down the project into very small and manageable units known as the sprints that produce a working version of a feature or a component. Agile model consists of 6 large steps that include Planning, Design and Development, Testing, and Deployment and Review. These cycles are repeated on the basis of response generated by all forms of users and changing needs to make the product progressively better day by day.

This project suits Agile especially well as the system will be refined and refined in small steps. This process is cyclical, leaving room where the user can interfere in the process at different intervals such that we will be able to make changes without having to rebuild the entire system afresh.

3.3.1 Planning

Planning Phase is the core of the whole project. It starts with an information-gathering exercise with all stakeholders, such as Admin, Staff at Student Affairs Division, and student requirement insight, to know their existing workflow and constraints in processing disciplinary records manually. Based on these early consultations, the overall user requirements are defined, i.e., student offence recording, case history, differentiation in role allocation, reporting, and secure access by students to their own records. The aim is to fully record functional requirements, what the system is to do, and non-functional requirements, how the system is to behave, e.g., to be secure, reliable, and simple to use. Once these are ready, they are ranked as a product backlog, which is an ordered list of features to implement.

This simplifies planning work over many sprints. A schedule for development is planned as a Gantt chart so that progress and milestones can be tracked. While they are doing this, the development tools are chosen and rolled out. These would be version control like GitHub, a local development environment on a machine with XAMPP, and other coding and test tools that are needed. There must be a plan that has been laid down by the development team at this point of completion that has set objectives, a timeframe, and resources needed to start developing confidently and planned.

3.3.2 Design and Development

During the Design and Development Phase, back-end code and the visual design start taking shape to develop the system. The phase begins with wire frames and mock-ups of interfaces which decide how the system will appear and how users will interact with it. Through these modelling, one can create particular interfaces to both Admin, Staff, and Student user roles, such as the login page all the way to case forms and dashboards. Responsiveness, clarity, and accessibility are also given special consideration in order to ensure that even non-technical personnel within the organization can go through the system with ease. MySQL database will be used to store user roles, files of disciplinary cases, timestamps, and the records of case history in a secure manner. The correct associations are made among tables so that the information flow is possible with no redundancy and to provide access control among tables to each user role where the students can see only their cases and the staff cannot remove the records.

After the design is approved, the system is created in small units referred to as sprints. Every sprint is dedicated to the creation of a particular feature or a module. As an example, the first sprint can be the implementation of the secure login and the second factor authentication, and the next sprint can be the disciplinary case reporting form which is used by the staff. It is developed with the help of PHP and MySQL as the backend and database, respectively, to provide high-level server-side code and stable data storage. The frontend is created with the help of HTML, CSS, and JavaScript in order to provide a user-friendly and responsive interface. This iterative development, continuous testing and feature-smooth integration approach is supported by this modular sprint-based approach. Security is implemented here with the help of password hash, input validation and SQL prepared statement that protects the system against vulnerabilities of SQL injection, unauthorized access and tampering with the form. CSRF token enforcement should be suggested as an improvement in the future. Demo and feedback by the supervisor and stakeholders are taken after each sprint and improvement of each iteration is made with the previous one.

3.3.3 Testing

Testing Phase is high priority to ensure that the system functions as desired, that it meets its requirements, that it has high degree of security and that it is user-friendly. During the development, testing is not limited to the end, but done continuously during its development. Unit testing in which individual features like the data submit actions, form validation, and the login mechanism are initially tested individually. This is to make sure that every module is functioning as expected and then they are incorporated in other modules. This is followed by integration testing, which is aimed at finding out whether the various modules of the system integrate smoothly without hitches. As an illustration, the discipline case module should be able to communicate efficiently with the student database, roles and generation of reports.

There is also the area of security testing which is significant here. SQL injection and unauthorized access attempts, improper session management, and so on are the security flaws that will be tested in the system. The input validation will also be scrutinised to ensure that malicious or malformed information is not posted in by the users. The User Acceptance Testing (UAT) would then be added as part of the technical testing by the selected representatives of all the user groups (Admin, Staff, and Students). These users will be tested on the system in an environment that is not live and give feedback on the layout, responsiveness and functionality of the system particularly confirming their particular access permissions. This feedback will enable the developer to learn how the actual users experienced the system and consider such a case to enhance the usability and overall effectiveness of the system to the individual user roles. Bugs, errors, and design problems found at this stage will be reported, fixed and re-tested before the deployment.

3.3.4 Deployment and Review

During the Deployment and Review Phase, the system is developed and is ready to be used. One last testing is conducted to reveal whether all functionalities are sound and there are no critical bugs in the system. After verification, the system is installed in a local environment, with the aid of XAMPP, which offers a secure and controlled environment to demonstrate and test the system. User documentation processes like administrator documentation, staff documentation, and student access documentation are also made at this point to enable the users to know how to use and maintain the system. With these resources, all stakeholders will be informed of the functions of the system hence using it effectively.

A post-deployment review is also done with client and supervisor to assess the result. This will entail introducing the system, how it will fulfil the initial requirements and areas which can be improved. The result of this session is recorded and taken into account in the further improvements, including the use of the encryption of the traffic with the help of the use of the SSL and automatic backups of the database and the connection with the attempts of institutional authentication. Agile development process is also reflected on in the review with successes, challenges, and some learnings. This reflection method guarantees the constant advancement of practice development and project management in the future.

3.4 Conclusion

Agile methodology is a suitable and efficient methodology that has been applied in the development management of the Secure Student Disciplinary Record Management System. It has a high focus on feedback, participant involvement, and iteration, which fits this project, which is associated with sensitive data, and unique user requirements of Admin, Staff, and Student, in intricate workflows. The system can be built step by step by breaking down the work into four steps namely Planning, Design and Development, Testing, and Deployment and Review with each step contributing towards an increasingly developed and functional end product.

In all these steps, such vital factors like security, usability and compliance have been considered. The Planning Step was used to ensure the right goals and requirements were set. The Design and Development Phase was to design the system in a secure, modular as well as an intuitive manner. The Testing Phase ensured that everything was functionality working as per and safely, and the Deployment and Review Phase ensured that the system was adequately prepared to be deployed to a live environment. All in all, the application of Agile not only has kept the project clean and on track but it also has made the final product technically stable and capable of satisfying the needs of its ultimate user in the context of the academic setting.

4 REQUIREMENTS

4.1 Introduction

In this chapter, the most critical Secure Student Disciplinary Record Management System requirements are described, how they are obtained by separating what the system must accomplish (functional requirements) and how effectively it must accomplish it (non-functional requirements), and what hardware and software is required. The objective is to develop a distinct and thorough foundation to direct the design and implementation of the system, in a manner that it genuinely meets the problems encountered and fulfils the needs of all its users.

4.2 Data Gathering Techniques

To ensure the proposed system actually addresses the requirements and challenges Universiti Poly-Tech Malaysia (UPTM) faces when dealing with student disciplinary records, a multi-faceted approach in data collection was applied. This integrated the use of quantitative and qualitative means of data collection to obtain information from the primary stakeholders.

To begin with, a Questionnaire was prepared and sent to a majority of the students through a Google Form. The questionnaire contained 11 ordered questions in order to assess student familiarity with current disciplinary procedures, concerns about data confidentiality through current manual practices, and what they would expect from greater transparency and security in their disciplinary case handling. The responses were gathered anonymously in an effort to make it easier to get honest and unbiased views, presenting a snapshot of the sentiments and requirements of the students.

Second, there was a formal Interview with an important client representative which is Tuan Haji Yahya bin Musa, Senior Manager for the Student Affairs Division (HEP) of UPTM. It was conducted via WhatsApp text, whereby it was easy and documented. The primary aim was to acquire a full appreciation of the present manual handling procedure of disciplinary cases, determine definite operating inefficiencies, and realize direct requirements for computerized systems by the principal administrative users. His experience was most beneficial to create the inherent functionality of the system and validate the inherent necessity for automation and increased security.

4.3 Functional Requirement

Functional requirements define the specific actions and capabilities the Secure Student Disciplinary Record Management System must perform. These are categorized by the distinct user roles: Admin, Staff, and Student.

User	Requirement	Description
Admin	Admin Access & System Control	• The system shall allow the Admin to securely log in, access a comprehensive dashboard, and manage all system-wide settings and configurations.
	User & Role Management	• The system shall enable the Admin to manage all user accounts (Staff and other Admins), including adding, editing, deactivating users, and defining their roles and permissions.
	Student Profile Management	• The system shall enable the Admin to add new student profiles and update existing student information.
	Full Disciplinary Case Management	• The system shall allow the Admin to create, view, edit, and delete any disciplinary case record, including managing statuses, outcomes, and evidence.
	Comprehensive Reporting & Case Tracking	• The system will allow the Admin to create professional reports (e.g., summary of misconduct cases, disciplinary trends, and records of how the staff cases were handled) in the form of PDF files. Automatic generation of reports on the request of the user assembles the case data in a printable format. Besides that the system will also facilitate case status (Open/Closed) in order to offer accountability and transparency in the disciplinary management.
Staff	Staff Access & Case Operations	• The system shall allow Staff to securely log in, view a dashboard, create new disciplinary case records,

		view existing cases, and edit/update their details (e.g., status, outcomes, evidence).
	Staff Deletion Restriction	• The system shall prevent Staff from deleting any disciplinary case records.
	Staff Notifications	• The system shall provide Staff with notifications regarding case updates or pending approvals. (This feature is proposed as future work.)
Student	Student Access & Own Record View	• The system shall allow Students to securely log in and view only their own personal disciplinary case records.
	Student Data & Action Restrictions	• The system shall prevent Students from viewing other students' disciplinary cases or from adding, editing, or deleting any disciplinary case records or administrative functionalities.
General System Functions	Search & Filtering	• The system shall provide a search and filtering mechanism for disciplinary cases based on various criteria (e.g., student name, ID, offense type, status).
	Printable Report	• The system shall generate printable reports in various formats (e.g., PDF).
	Case Status Tracking	• The system will keep a record of disciplinary cases, statuses (e.g. Open or Closed), this will enable Admin and Staff to filter and control cases in relation to whether closed or open.

Table 2: Functional Requirement

4.4 Non-Function Requirement

Function	Result
Security	• The system will incorporate secure user authentication with hashing of passwords (Bcrypt) and differentiate controlled access control of all the users based on their roles. • The system will be resistant to typical web attacks such as input validation and SQL prepared statements to minimize threats of SQL injection and basic XSS attacks. Limited access and role-based visibility can help adhere to the requirements of the Personal Data Protection Act (PDPA 2010) in Malaysia. Future improvements suggested include the use of an encryption mechanism (SSL/TLS) and a token system (CSRF) to implement institutional deployment.
Usability	• The system will be user-friendly with intuitive and easy to navigate user interface across all user roles that will include clear error-messages and feedback. • The system will contain a detailed user manual (admin, staff, and student manuals).
Performance	• The system shall load pages and display the search results within 3 seconds, and efficiently handle a minimum of 50 concurrent users.
Reliability	• The system shall maintain 99% availability during operational hours, implement daily automated database backups, and recover from failures within 1 hour.
Scalability	• The system will be able to support the growing size of data (student records, cases) and a number of users (Admin, Staff, Students) without major system architecture modifications.
Maintainability	• The system code shall be well-structured, modular, and commented for ease of future maintenance, and developed using widely supported technologies and frameworks.

Table 3: Non-Functional Requirement

4.5 System Requirement

The following section will describe hardware and software minimum requirements needed to develop and possibly implement the Secure Student Disciplinary Record Management System.

4.5.1 Hardware Requirements:

- Development Machine:
  - Processor: Intel® Core™ i5-10500H (2.50GHz) or equivalent
  - RAM: 8GB GDDR6 (minimum)
  - Storage: 512GB HDD (minimum)
  - Display: 15.6-inch Full HD (1920x1080)
  - Network: Stable Wi-Fi internet connection
- Deployment Server (Proposed):
  - Processor: Quad-core CPU (minimum)
  - RAM: 16GB (minimum)
  - Storage: 500GB SSD (for faster I/O)
  - Network: High-speed internet connection, dedicated IP address

4.5.2 Software Requirements:

- Operating System: Windows 10/11 (64-bit) for development; Linux-based OS (e.g., Ubuntu Server) for deployment.
- Frontend Technologies: HTML5, CSS3, JavaScript
- UI Framework: Bootstrap 5
- Backend Framework: PHP (custom implementation)
- Database Management System: MySQL; phpMyAdmin (for database administration)
- Web Server: Apache or Nginx (for deployment)
- Development Tools (IDE & Version Control): Visual Studio Code, Git, GitHub
- Local Development Environment: XAMPP (for Apache, MySQL, PHP) or similar environment.

4.6 Conclusion

The requirements of the Secure Student Disciplinary Record Management System have been well defined in this chapter. Rigorous data collection procedures like questions and interviews have been used to explain non-functional and functional requirements. These are necessities by a few functions of the user such as Admin, Staff and Students, as well as the necessities like a good design, usability and performance, which will shape the design and development of the next iterations. The above system requirements will ensure that technical infrastructure is provided to come up with a stable and effective solution.

5 ANALYSIS

5.1 Introduction

This chapter gives an in-depth examination of the information collected during the requirements process, converting raw data into meaningful findings to inform the design of the Secure Student Disciplinary Record Management System. It combines data from interviews and questionnaires, and subsequently represents the structure of the system and its processes graphically using a Use Case Model and Flowchart. This examination creates the overlap between knowledge of the problem and envisioning the solution so that system design is stable, easy to use, and right for the needs of the university.

5.2 Data Gathering Analysis

Analysis of data from interviews and questionnaires yielded valuable information on the present issues of handling student discipline records and the particular requirements for a computer intervention.

5.2.1 Questionnaire Analysis (Pre-Development)

Student questionnaire was useful in terms of demographic data and understanding of recognition and anxiety among students. It was revealed that the majority of the students know about the university disciplinary process, though to a lesser degree, and the number of students who are not aware or do not know is huge, thus requiring a better means of communication and access. Concern about the fact that their personal and disciplinary information could be distributed as confidential and safe in the existing manual system also demonstrated the high level of concerns of the students. The need to comply with PDPA was seen in the fact that the system needed to have high levels of security, effective data accuracy and open audit trails by the students. Moreover, the recommendations of the students included the optimization of the case handling process, which meant that the cases of discipline disposition should be faster and more transparent. The findings had direct impact in the incorporation of safe access by the students of their own records and concentration on applying efficiency in designing the system.

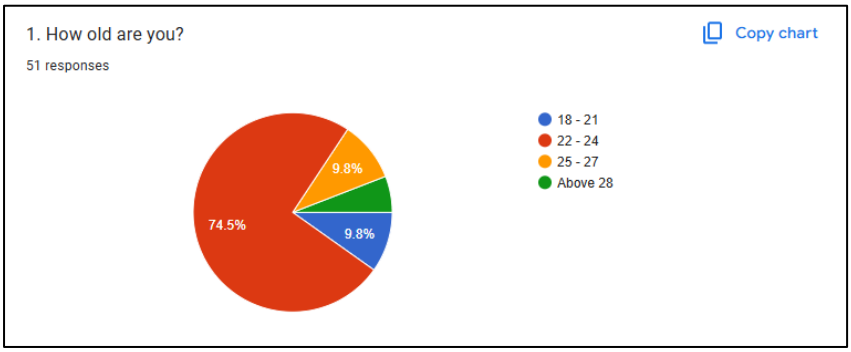


Figure 5: Question 1

The majority of respondents, 74.5 are within the 22-24 age bracket and therefore the survey was actually representing the perception of young adult students. The other respondents were evenly distributed at 18-21 (9.8%), 25-27 (9.8%), and above 28 (5.9%), and gives a demographics picture of how the student population is age-distributed.

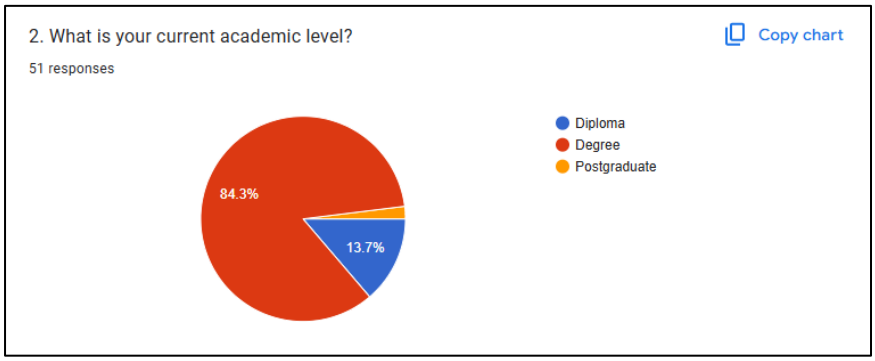


Figure 6: Question 2

The questionnaire largely surveyed Degree students, who comprised 84.3% of the reply. 13.7% of the reply was from Diploma students with a small Postgraduate student reply at 2%. This split verifies that the information collected properly includes undergraduate student opinions and experiences at the university.

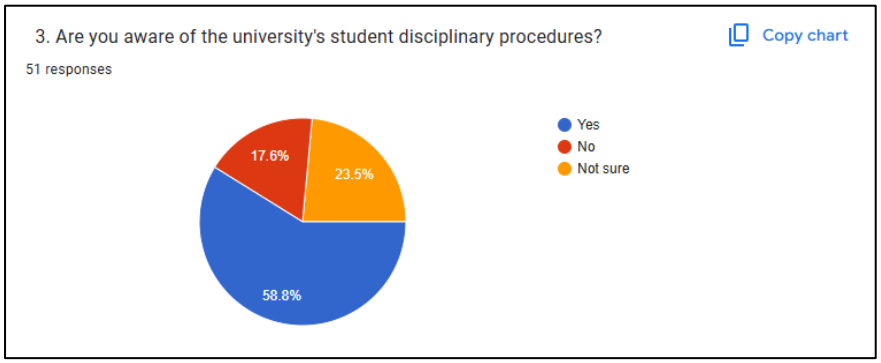


Figure 7: Question 3

An overwhelming 58.8% of students reported they knew the university disciplinary procedure. But 17.6% did not know at all, and 23.5% were unsure, demonstrating a very clear need for increased communication and accessibility to these procedures.

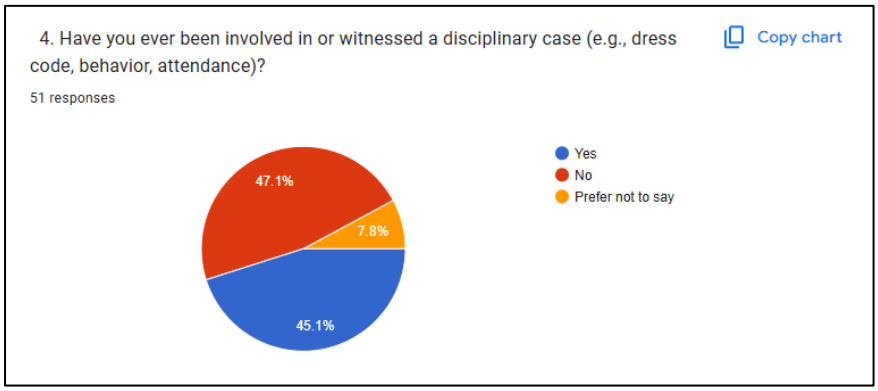


Figure 8: Question 4

Almost half the respondents, 45.1%, said they had been a party to or witnessed a disciplinary case. A total of 47.1% had not, and 7.8% didn't feel like saying, so discipline is a visible component of the student experience for quite a few of the university population.

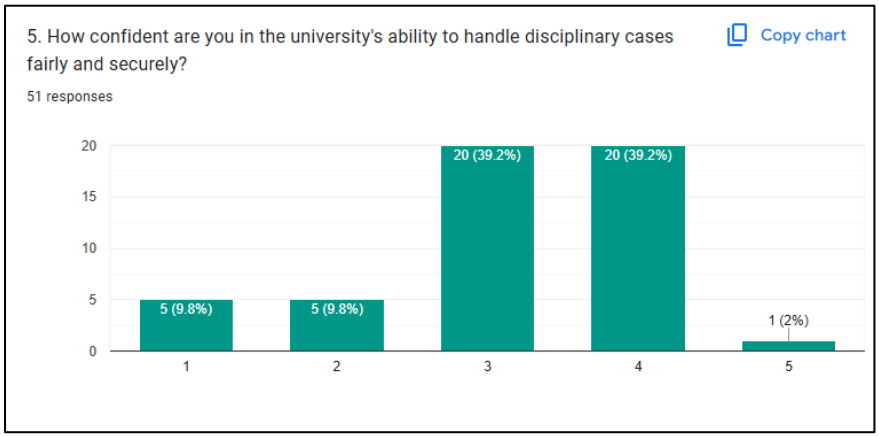


Figure 9: Question 5

Student confidence in the university case handling also varied, with the biggest groups (39.2% each) being neutral '3' or just more confident '4' out of a 1-5 scale. A lesser group (9.8% each) were low-confidence ('1' or '2'), while only 2% were full confidence ('5'), reflecting a potential for improvement in building confidence in fairness and security.

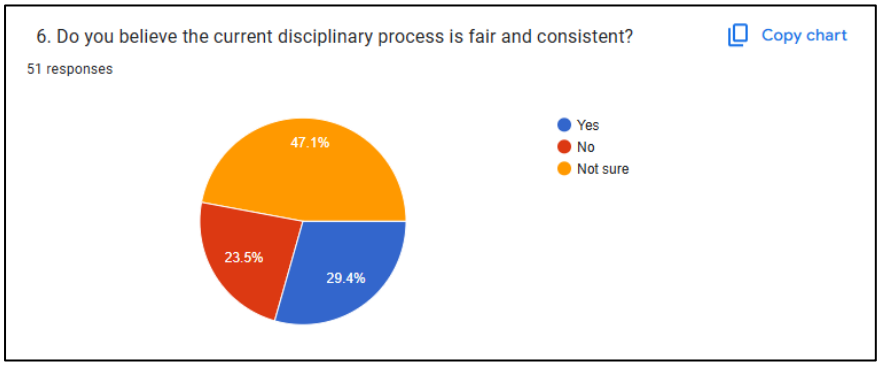


Figure 10: Question 6

Student views about the fairness and consistency of the existing disciplinary process were mixed, with 47.1% being unsure, 29.4% viewing it as fair and consistent, and 23.5% viewing it as unfair and inconsistent. This indicates a gigantic perception gap and uncertainty among students about the uniformity and fairness of disciplinary action.

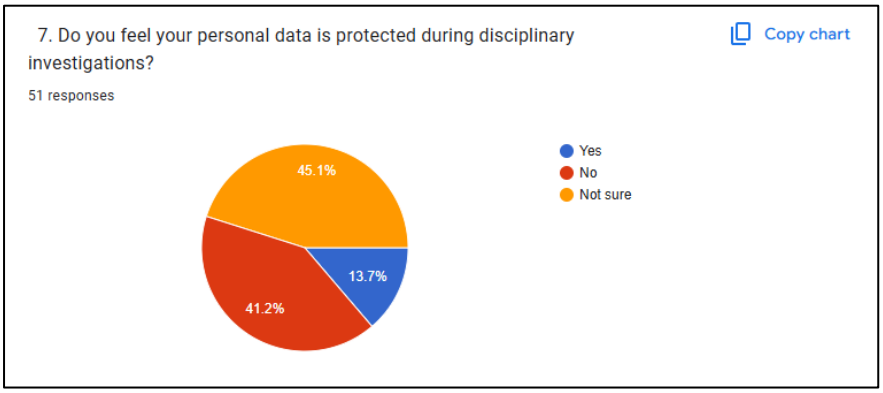


Figure 11: Question 7

An astonishing 41.2% of the students believed that their personal information was not safeguarded in investigations, with 45.1% doubting and only 13.7% of them certain that it was safeguarded. This positive indicator of doubt or non-safeguarding reflects a serious concern of privacy that needs to be addressed with the suggested system.

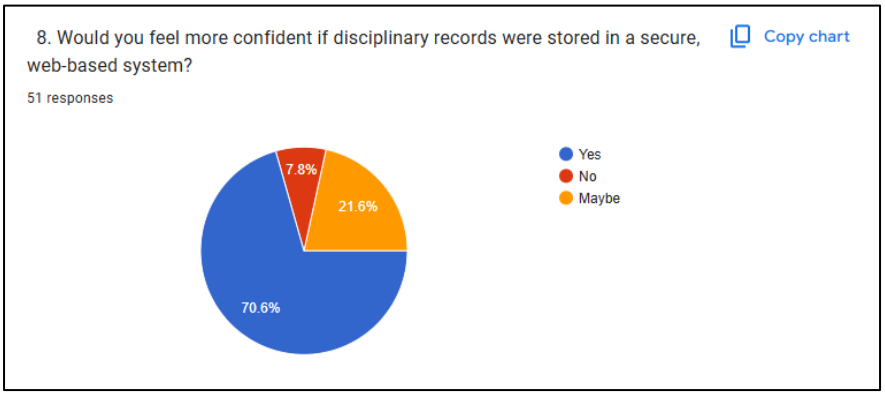


Figure 12: Question 8

The percentage of the students answering yes was very high 70.6% because they need to be more certain in case there are disciplinary records stored within a secure web-based system. 7.8% answered no, and 21.6% answered possibly which indicates that students have a great deal of support regarding having a digital solution in building confidence with data security.

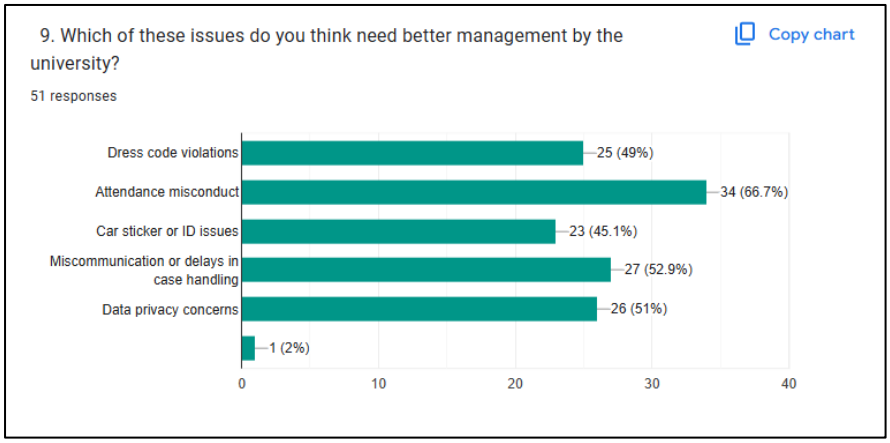


Figure 13: Question 9

There are several points of concern mentioned by students that require a better approach: car sticker or ID issues (45.1%), delays during communication or case processing (52.9%), data privacy (51%), and violation of the dress code regulations (49%). 66.7% also noted the presence of attendance misconduct, and it indicates the overall breadth of changes in the administrative and communication processes.

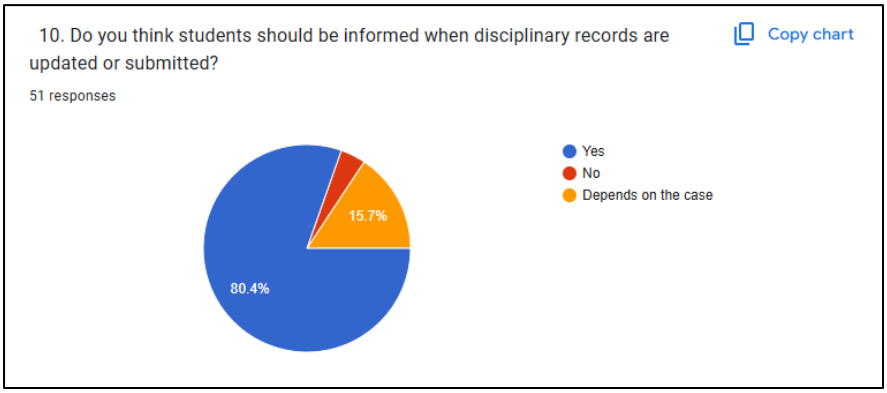


Figure 14: Question 10

The overwhelming majority of students, 80.4% have said that they would like to know when disciplinary records are updated or sent, 3.9% have said no, and 15.7% have said that it depends on the case, which again points to the fact that there is high demand in terms of greater transparency and timely reporting by the university on their disciplinary status.

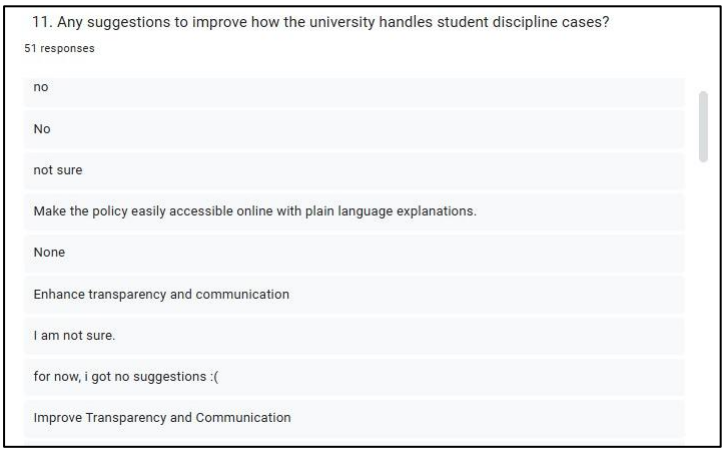


Figure 15: Question 11 - Part 1

Other students did not have any particular suggestions, as some of them said no or none. But most other people would really like the university to be more open and transparent on the way discipline handling is done. They want the policies to be more accessible online and in the easily understandable language because every person should know what is happening. It is everything that makes things less complicated and simpler.

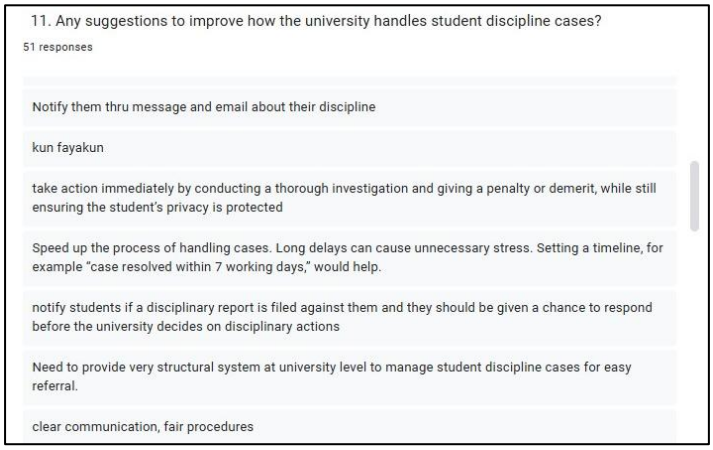


Figure 16: Question 11 - Part 2

This category of feedback was very demanding in terms of faster activities and improved communications. Students desire to know immediately (through a message and email) when a discipline report is registered against them and have an opportunity to present their version. They are fed up waiting, they want cases to be fast-tracked, possibly in a period less than a week, to relieve stress. They are simply seeking an appropriate, structured mechanism to have things running.

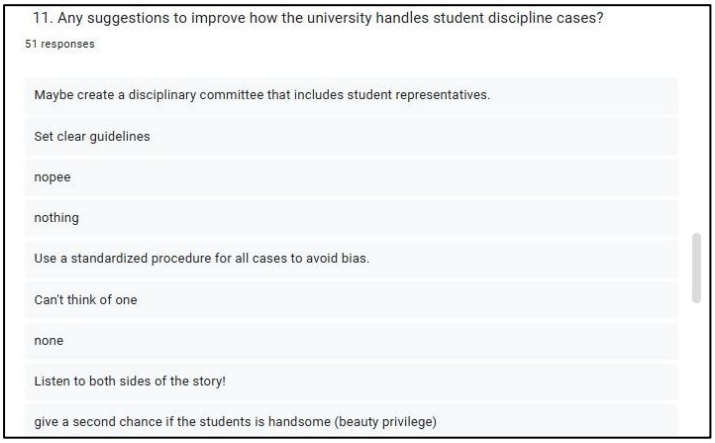


Figure 17: Question 11 - Part 3

In this case, the students were quite concerned with equality and uniformity. They would prefer that the university treat all in a similar manner so that it does not favour anyone. They further emphasized on the need to hear both sides of the story in order to ensure that decisions are equitable. There were even recommendations of having students in the disciplinary committee so that it could be balanced.

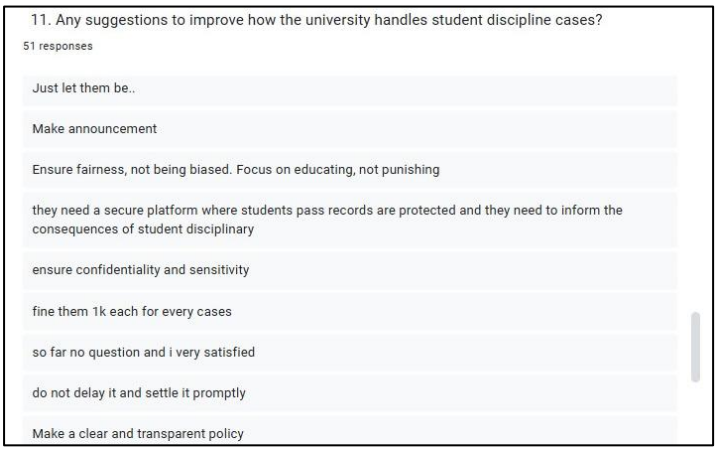


Figure 18: Question 11 - Part 4

This part paralleled the desire to have some privacy and fast and decisive action. There is also a concern among the students that their personal discipline history may leak out, hence they desire a safe location to keep records. They called upon the cases to be done promptly and the policies to be very clear. Another good thing was the fact that discipline is more about providing lessons to the students rather than merely punishing them.

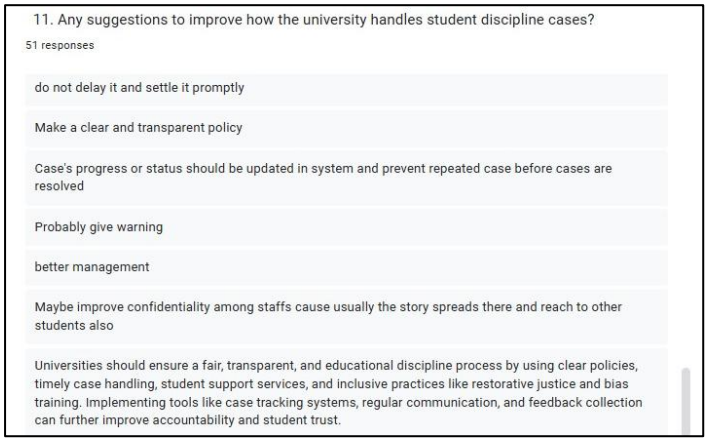


Figure 19: Question 11 - Part 5

Lastly, all these recommendations tied it all. Students would like to see case updates within a system, as they are aware of what is going on, and they do not want to repeat the same troubles in the future. One of the major issues was employees discussing cases and the leakage of information, which actually points to the necessity of a safe and confidential system. Finally, students desire a fair, open, and a disciplinary process that assists them to learn, and not only punish.

5.2.2 Interview Analysis

Figure 20: Tuan Haji Yahya bin Musa (Senior Manager HEP)

The main data of the existing working problems were collected through the interview with Tuan Haji Yahya bin Musa, Senior Manager of UPTM Student Affairs Division (HEP). He confirmed that discipline cases are processed mainly by hand based on physical records, which causes major problems such as risk of high data loss, slow retrieval of previous records and high risk of privacy.

Tuan Haji Yahya emphasized a number of peculiarities the digital system should possess by the Student Affairs Division:

- Integrated student profiles for comprehensive information.
- Status tracking for real-time updates.
- Auto-generated warning letters to standardize communications.
- Robust report and statistics generation for data-driven decision-making.
- Differentiated role-based access with secure login to protect sensitive information.

Crucially, he expressed strong support for the project, indicating that the client is open to becoming an official system client and providing ongoing feedback. This strong client backing is a significant asset for the project's success and ensures the system's development is aligned with real-world operational requirements.

5.3 Use Case Model

The Use Case Model graphically depicts the essence functionality of the system and how the main user functions relate to each other. In order to get a more focused and more concise view of the perspective of each individual user, the general use case model has been divided into three different diagrams to each of the main actors: Admin, Staff, and Student.

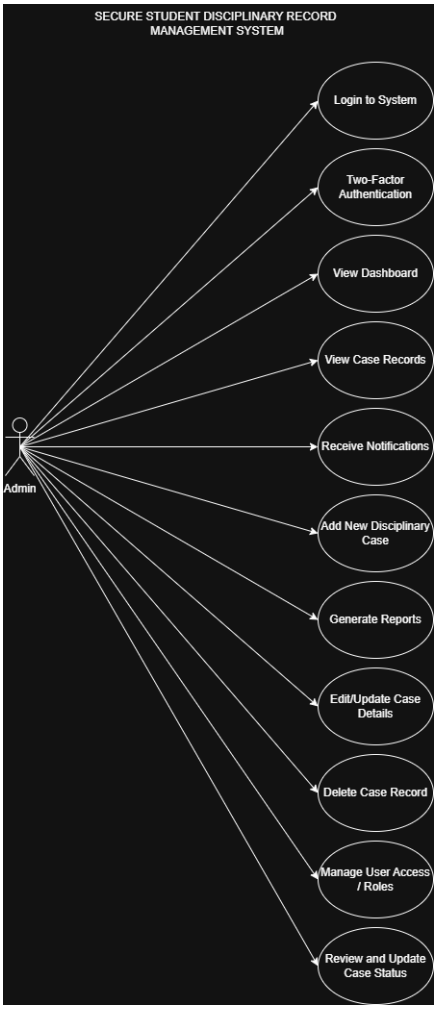


Figure 21: Use Case Diagram for Admin Module

The control of the system is maximum in the Admin actor. Admins are able to securely log in using Two-Factor Authentication (2FA) and control every bit of the platform. They are Manage User Accounts (add, edit, deactivate Staff and Admin accounts), Manage User Roles and Permissions, and Manage Student Profiles. Create, View, Edit and Delete Disciplinary Cases are also used by admins dealing with disciplinary cases. Moreover, they are able to Generate Reports and change System Settings. The combination of these capabilities indicates the role of the Admin who is the general controller of the system, to assure adequate governance and security. The 'Receive Notifications' use case is meant to accommodate real time notifications but is an upgrade of the future.

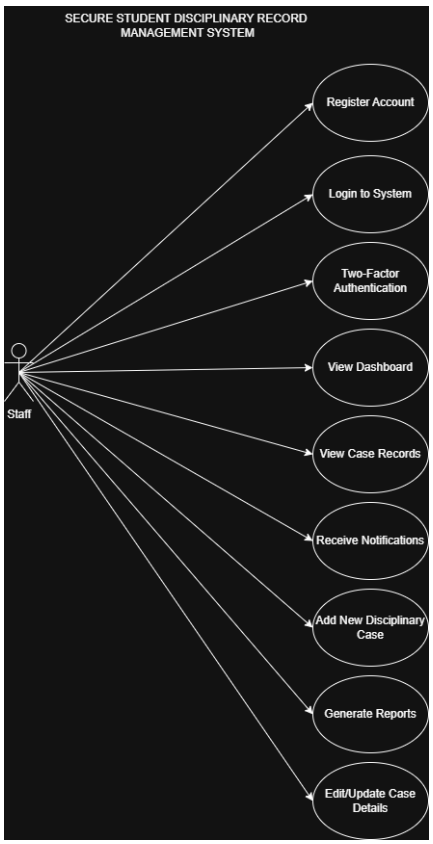


Figure 22: Use Case Diagram for Staff Module

Staff actor is able to Register Account and to be a part of the system and then to Login with Two-Factor Authentication (2FA). Their primary functions are Create Disciplinary Case (new record creation), and View Disciplinary Case and Edit Disciplinary Case which are used to manage the existing records. The Receive Notifications use case was taken into account in terms of design to make the staff aware of the case developments, yet, this issue was not implemented in the given version, and it is suggested as a future work. In general, the Staff module is dedicated to the daily day-to-day case management tasks to sustain the transparency and efficiency.

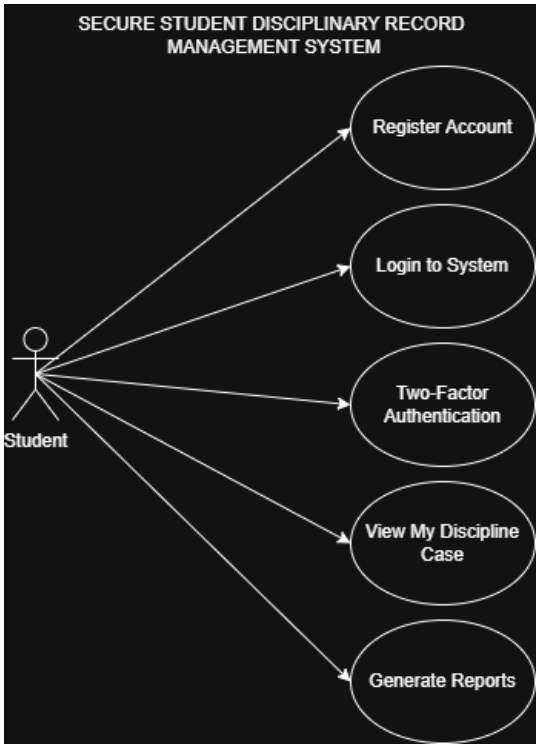


Figure 23: Use Case Diagram for Student Module

Student actor is able to Register Account and safely use Two-Factor Authentication (2FA). After authentication, students can see their own Disciplinary Case records, which are transparent and at the same time not very confidential. They are also able to produce the reports of their disciplinary records so that they can be able to download official documents when they need them. Such minimal and necessary functions are sufficient to provide students with safe and role-based access to their personal information and to avoid the unauthorized access to the personal data of other students.

5.4 Flowchart

The following flowcharts show the main process of the Secure Student Disciplinary Record Management System as it exists with the different user roles of an Admin, Staff and Student: Such diagrams provide flow of processes and decision points that the users go through when interacting with the system. Each of the flowcharts starts with safe entry processes, such as Two-Factor Authentication (2FA) and proceeds to the list of activities that each position is allowed to do. With the visualization of these flows, the logic of the system would better be understood and grasped and role-based access and functionality should be properly applied.

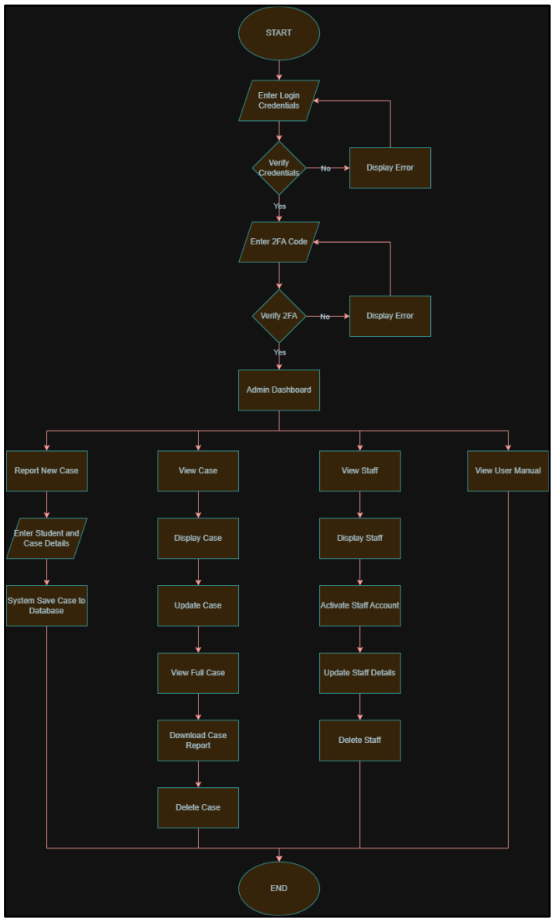


Figure 24: Flowchart for Admin - User Management Workflow

This flow chart will define how the Admin will handle user accounts. Once logged in and through Two-Factor Authentication (2FA), the Admin is redirected to the dashboard and chooses the user management module. At this point, the Admin would be able to either create a new staff account, modify the current staff information, or delete a staff account. Every action will result in a confirmation step and then the system will update the database. Such flow allows sensitive user management to be conducted by authorized administrators, keeping systems intact and in control.

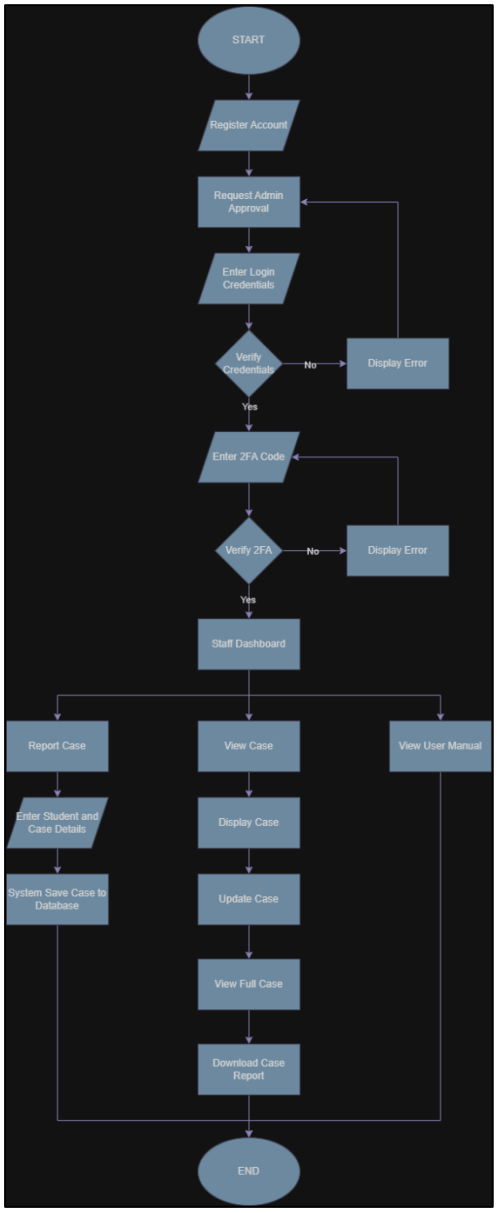


Figure 25: Flowchart for Staff - Incident Reporting Workflow

This flow chart identifies the course of action that a Staff member will adhere to in order to report a disciplinary case. It starts by registering an account, proceeds through Admin approval, into login and 2FA verification. After authentication, the Staff is allowed an access into the dashboard and he/she chooses Report Case. They fill details of the student, explain what happened and post evidence supporting the case and send it in. The case is then stored within the database by the system. This orderly flow of work makes sure that the disciplinary cases will be recorded and safely stored to be reviewed and taken into action.

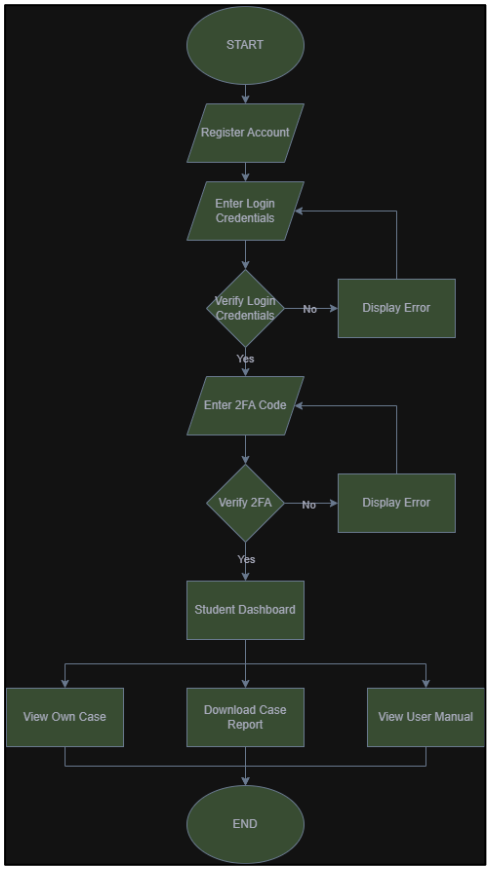


Figure 26: Flowchart for Student - View Own Disciplinary Record Workflow

The following flowchart illustrates the access of disciplinary records by a Student. Once having registered an account, the Student logs in and does 2FA verification. After authenticating successfully, they are joined to the Student Dashboard where they can access the disciplinary matters of their own, download case reports, and the user manual. In case there are no records, the system will show a message that no cases of discipline are located. Such flow guarantees the transparency of the program and high privacy rates so that only personal records of students are accessible.

5.5 Conclusion

The vision of the requirements and conceptual design of the Secure Student Disciplinary Record Management System have been established in this chapter on analysis. The analysis of data retrieved as a result of interviews and questionnaires has helped to identify the main problems and exact user needs. The Use Case Model briefly explains how the Admin, Staff, and Student would interact with the system functionality, whereas the Flowchart explains the procedure with minimum steps to deal with disciplinary cases. The new and elaborate analysis is an initial prerequisite and therefore the design and development processes henceforth will lead to a system that will be safe, efficient, user-friendly and fully compatible with the operational need of Universiti Poly-Tech Malaysia (UPTM).

6. DESIGN

6.1 Introduction

The design plan of the Secure Student Disciplinary Record Management System is this chapter. It helps to fill the gap between the theoretical requirements and the actual way of implementation, providing a precise plan on the system development. In this section, the design decisions made on the interface of the system, the physical and logical database structure, and the security mechanism that is important and that helps in each and every operation of the functionality will be recorded in details. The architecture has been built on a secure and iterative development practice in an endeavour to make sure that the final product is resilient, easy to use and able to process sensitive information in the most ideal integrity and confidentiality.

6.2 Interface Design

The UI was created with a very heavy emphasis on simplicity, usability, as well as, role-based access. The visual basis of the UI, wireframes, were designed with much attention to consistency and effectiveness on various pages to attract the users. It was aimed at developing an interface which would lead a user with minimum friction through his/her particular actions, thus rendering the system easy to learn, and efficient to use. The system appears professional by coming up with a logical design language starting at the login page all the way to the dashboards. This allows making interactions more consistent and less cognitive overload so that users can concentrate on their actual work without worrying about using a complicated user interface.

The interface, in its various parts, is specifically designed with regards to the specific requirements of the respective users, that is, the Admin, Staff, and Student users, ensuring that each user is only presented with the information and features that are pertinent to them at any given moment. In the case of the Admin, the interface would be the hub of control where the users and the case records are handled in the system. The Staff interface is action based and designed to facilitate smooth running of adding and maintaining disciplinary cases. The interface of the student is clean, safe and they will only have a read-only access to their personal records; anything they do not need will not be provided. Such role-based system increases usability, and also serves as crucial, first-line, security measures to ensure that an unauthorised user cannot perform functions outside his or her role.

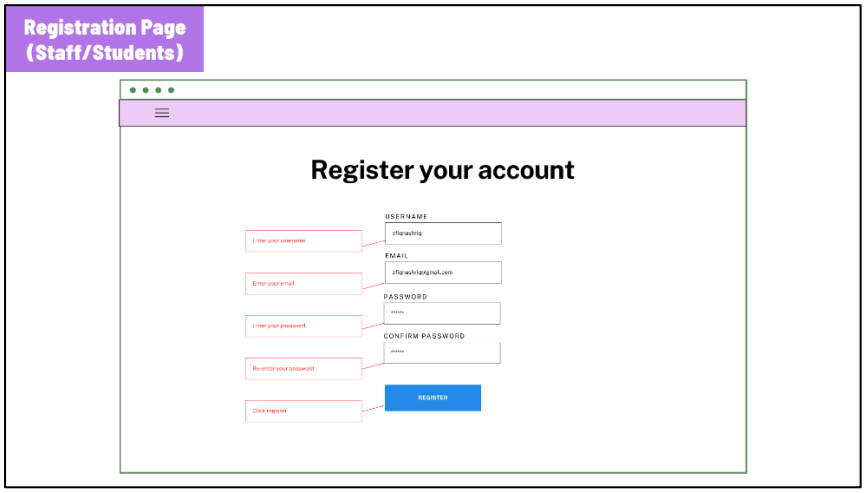


Figure 27: Registration Page

New staff and students can make an account in the system in the registration page. It demands personnel to register, giving it a username, email address, and password whereas students must be registered by giving it a username, student ID, name, email address, and password. Input checking makes certain that there may not be duplicates of accounts created and all the necessary fields filled in. This page helps in secure enrolment of users into the system.

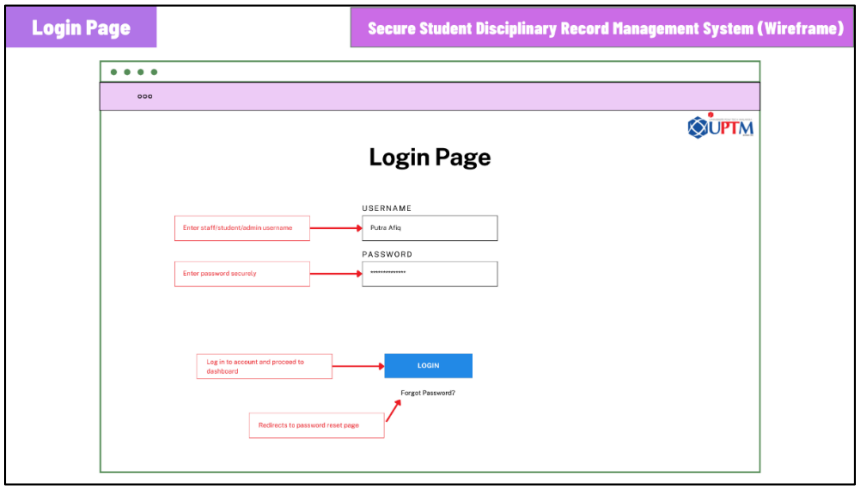


Figure 28: Login Page

The system has a login page that is the entry point of all users, including the users of the admin, staff and students. This has areas where the user and password are entered and there is a login button that allows one to safely access the system. There is also the link of Forgot Password, where the user can redeem their account in case they lose the login details. This page will also make sure that the disciplinary record system is only accessed by authorized persons.

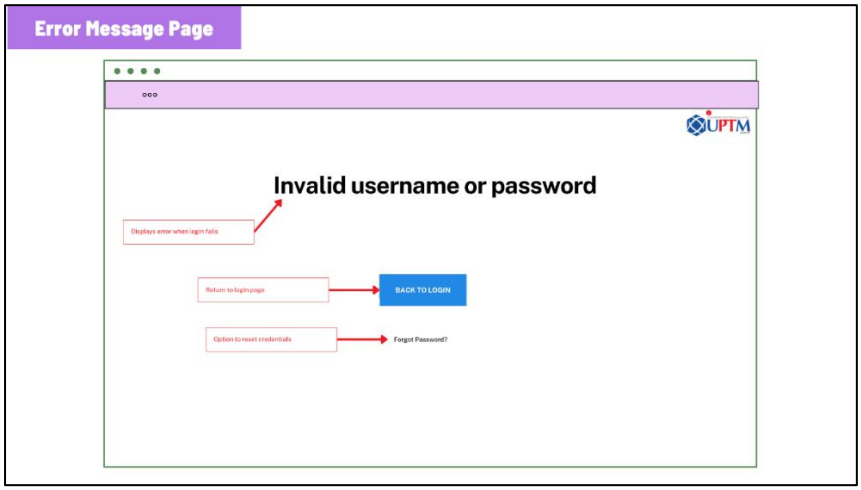


Figure 29: Error Message Page

In case the user key in the incorrect credentials, the error message page is opened. This provides immediate response to the user by displaying a warning of invalid login. This page allows users to restart all over again or reset their credentials with the help of the "Forgot Password" link. This aspect guarantees improved usability and unauthorized access.

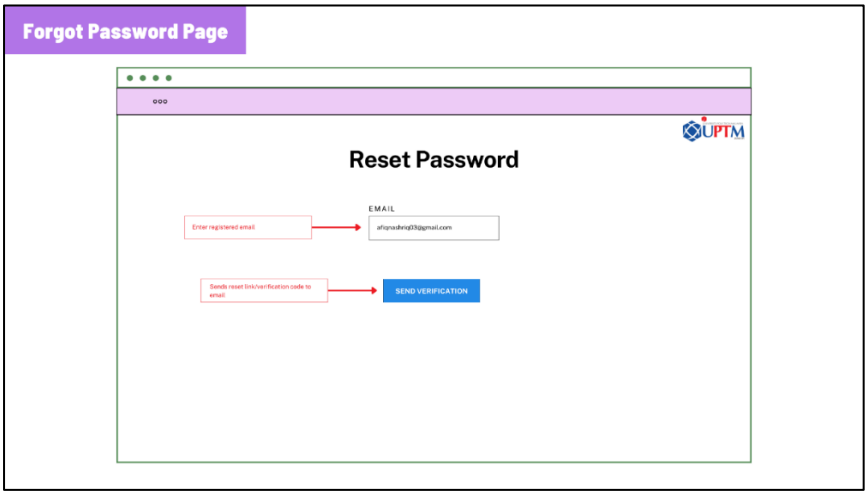


Figure 30: Forgot Password Page

The forgot password page enables users who cannot log on to the site to retrieve their accounts. This entails the user typing in his or her registered email address after which an email is sent to the user with a verification link or a verification code. After verification, the user is able to change the password and log into the account. This is a security measure that will make the accounts more secure and no employee or student can ever be permanently locked out of the system.

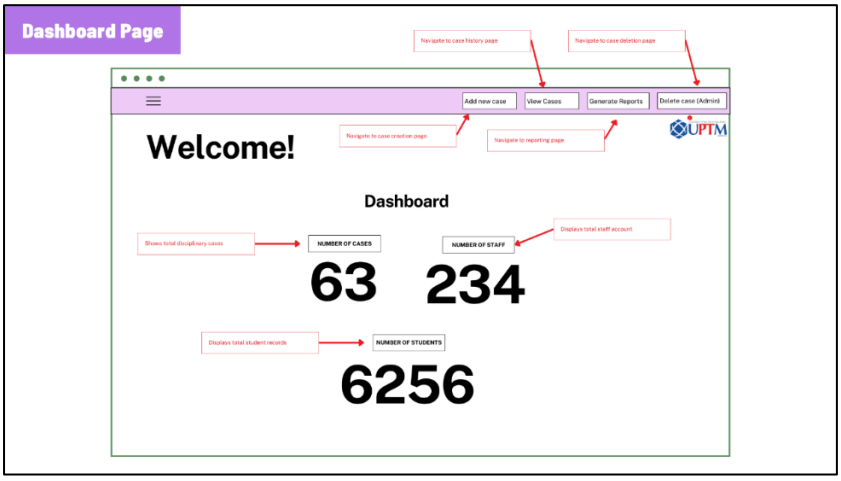


Figure 31: Dashboard Page

The dashboard is the center of the system, where the user can view and access the main functions quickly. The statistics of the number of admin, discipline cases, staff, and students currently in the system are also shown. On this, the user selects an action that shows case history, generates reports, user manual, or adds a new case. Admin can delete cases. This page makes it easier to navigate and get an overview of the status of the system.

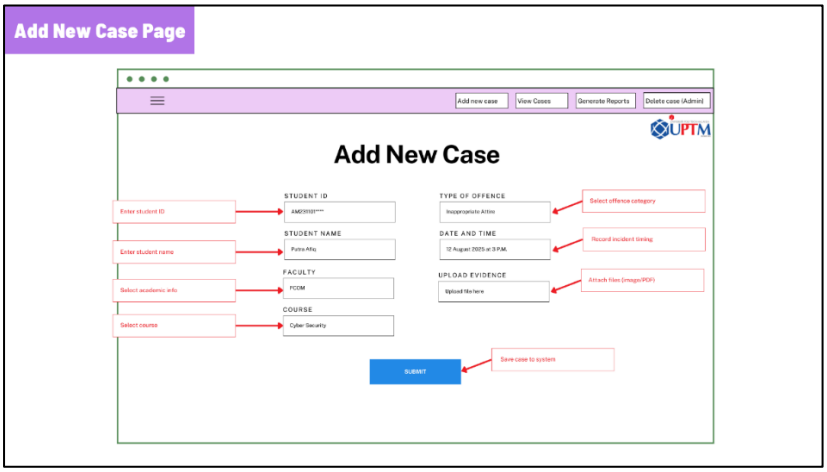


Figure 32: Add New Case Page

The add new case page allows staff to record a new disciplinary case against a student. Users can fill in detailed information, such as student ID, name, faculty, and course, plus specify the offence type and the date and time of the incident. Evidence such as images or PDF files can be uploaded to support the case. On submission, this form saves the case in the database for further review and action. This page ensures that all records are complete and well-documented.

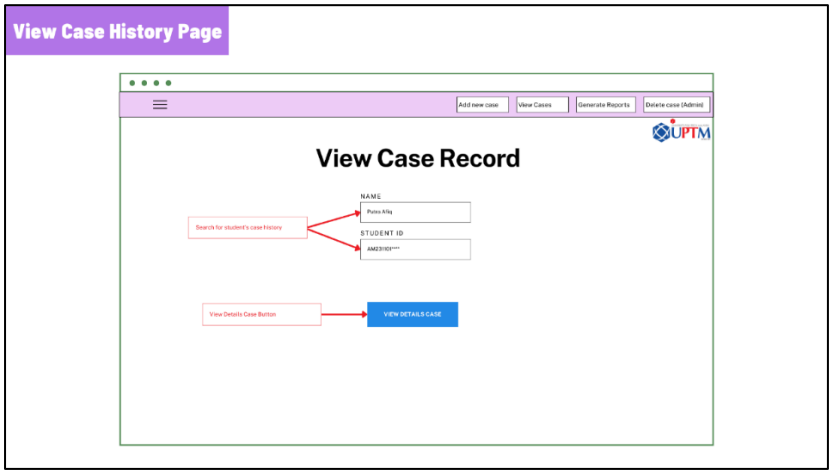


Figure 33: View Case History Page

The View Case History page helps the staff to search and see the existing disciplinary records of the students. After typing in the name or ID of the student, a list of cases associated to the specific student comes up and the staff can access detailed records of individual cases and take further action or go through them. The feature will help in tracing recurring offenses and keeping transparency in disciplining students.

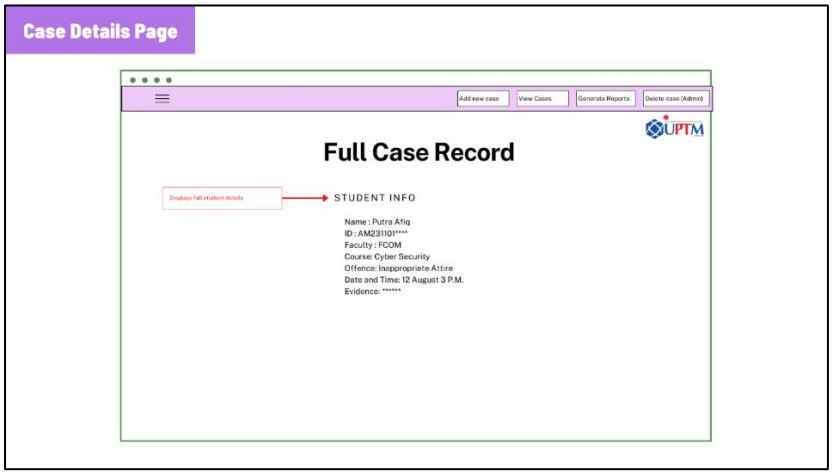


Figure 34: Case Details Page

A case details page provides all the details of a specific disciplinary case that include a personal information of a student, the type of the committed offense, the date and time of the event, and evidence that may prove it in case it is uploaded as a document or a photo. This makes staff to have a good glance at the case to ensure that nothing is amiss. Since it puts all the information in a single location, it allows the Student Affairs staff not to lose a vital piece of information when dealing with cases.

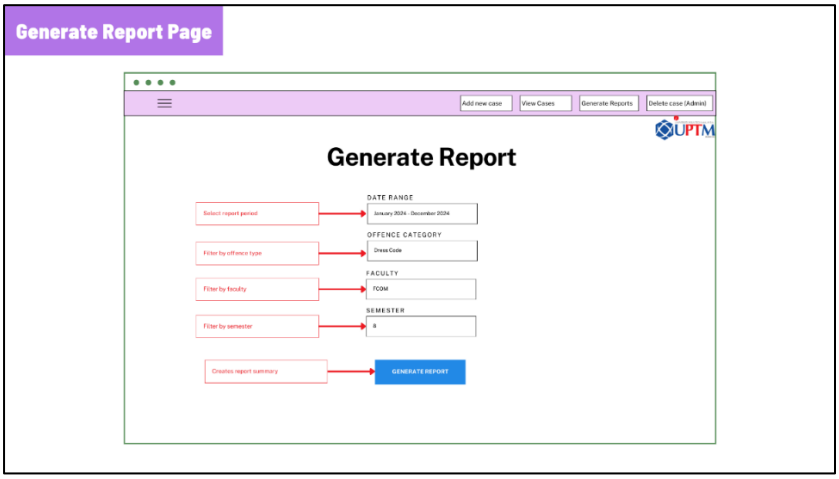


Figure 35: Generate Report Page

The Generate Report page can be used by the staff, administrators, and students to create summaries of the disciplinary cases. Having been created, the system automatically creates a structured PDF report based on the relevant case information, which may be utilized either to create formal documents or in-house to conduct an analysis. This saves man power, enhances accuracy and simplifies decision making by having a clear summary of disciplinary records.

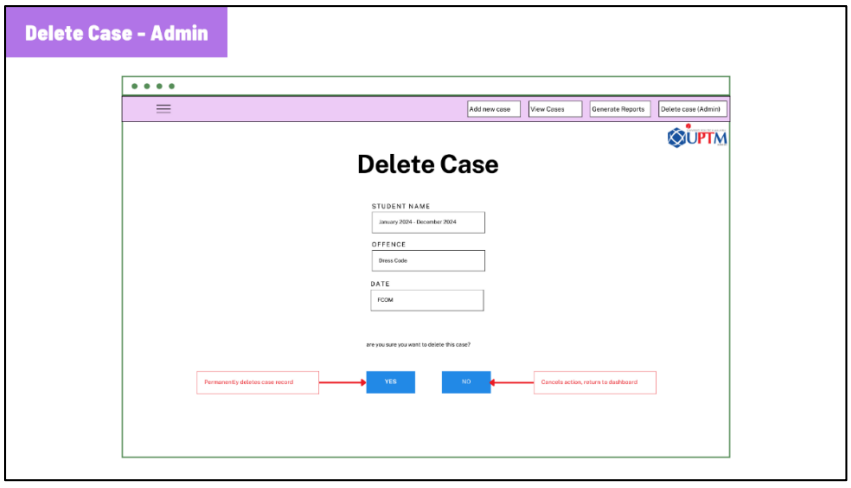


Figure 36: Delete Case (Admin) Page

Administrators are allowed to access the delete case page. It gives a choice of permanently removing the disciplinary case in the system. This page will also display the summary information on the chosen case to be deleted, such as the name of the student and data on his/her offence. The administrators are presented with an option of confirming deletion by clicking on a yes button or cancelling the option by clicking on a no button. This will ensure that there will be protection against accidental loss of information but the administrators will still have complete access to the records of the system.

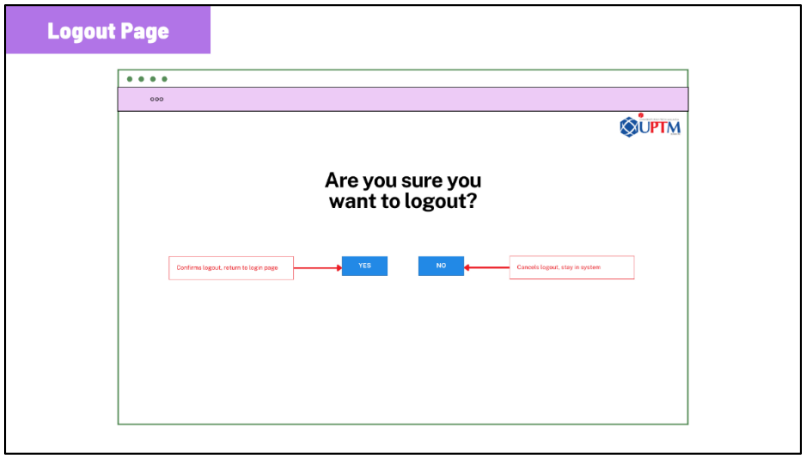


Figure 37: Logout Page

A user is informed when they decide to exit the system on the logout page. It will give two choices, one of them is yes to log out and go back to the login page or no to cancel and remain in the system. This feature is secure because it will automatically shut the active sessions and unauthorized use of the system in an unattended device.

6.3 Database Design

Database design is one of the important stages of the project since it involves organizing, storing and retrieving all the data required in the system. The rational organization of information is a guarantee of efficiency in activity and final stability of the system. The database structure of the Secure Student Disciplinary Record Management System will be uniquely developed in such a way that management of a large volume of sensitive information such as student credentials, case files, and case history records among others are supported by data integrity.

This design is centered on the data dictionary. It is a central repository of metadata that is a complete description of all the tables and fields of the database including data type and field size as well as what each attribute represents. It is taken as a general reference guide, which enables everybody to know what is meant by all the items of the database and what each one holds.

In a summary form, the ERD indicates the schema of the database. This diagram indicates the relationship between the various tables, including Student, Disciplinary_Cases and User. The ER diagram simplifies the connections among the data points to be more comprehensible with a graphical display of primary and foreign keys. It is highly significant in generating consistency in data and making effective queries. This model gives the plan of the design or interpretation of the data architecture of the system.

The Data Flow Diagram illustrates how the information flows within the system and how data that can be regarded as an input e.g., in this case, a staff member adding a new case or the student requesting their records is received, processed and converted. The DFD identifies data flowlines, the origin of data to the destination, and ensures that the entire data of processing data is in accordance with the main objective of the system that is to safeguard and access data on student disciplinary records.

6.3.1 Data Dictionary

Field Name	Data Type (Size)	Description
userID	int(11)	Primary key; unique identifier for each user
username	varchar(50)	Username used for login
email	varchar(100)	User's email address
passwordHash	varchar(255)	Hashed password for secure authentication
userRole	varchar(20)	Role of the user (admin, staff)
createdAt	datetime	Timestamp when the user account was created
status	varchar(20)	Account status (e.g., active, inactive)

Table 4: Data Dictionary of Table "Users"

This is the primary authentication and base roles table of all system users such as Admins and Staff. Every user is uniquely identified by a userID, as well as by login credentials in the form of username and email, and has a securely hashed password (passwordHash). The field userRole is what determines how far access to the system goes; whether Administrator, Staff, or Student by setting the role-permission access privileges. Timestamp createdAt records the date when the account is created, status represents the state of account: active or inactive.

This table is essential as regards to the secure access management: the system is configured to perform the functions of the login authentication, role-based authorization and administrative control over the user accounts. The system is modular by disconnecting user identity with student-specific data and increases security.

Field Name	Data Type (Size)	Description
studentID	varchar(20)	Primary key; unique identifier for each student
username	varchar(50)	Student's login username
email	varchar(100)	Student's email address
passwordHash	varchar(255)	Hashed password for secure login
userID	int(11)	Foreign key linking to users.userID
studentName	varchar(100)	Full name of the student
faculty	varchar(100)	Faculty the student belongs to
course	varchar(50)	Course enrolled by the student
semester	int(11)	Current semester of the student

Table 5: Data Dictionary of Table "Students"

The students table holds both academic and personal data of every student user. Each student is given a distinctive identifier known as the studentID and may be connected to the users table using the foreign key known as userID such that every and every student would be associated with a respective user account in order to log-in. This table has such fields as studentName, faculty, course, and semester that make the identification of students possible and, therefore, facilitates the filtering of cases in the disciplinary system.

This table is essential in making the association of the disciplinary case with each specific student. This provides the ease of students only being able to view their respective records and also to facilitate individualized dashboards and reporting systems. The fact that the data on the students and user credentials are separated is further supporting the elements of data privacy and adherence to PDPA.

Field Name	Data Type (Size)	Description
caseID	int(11)	Primary key; unique identifier for each case
studentID	varchar(20)	Foreign key linking to students.studentID
caseDate	datetime	Date the incident occurred
caseTime	time	Time the incident occurred
offenseType	varchar(50)	Type/category of the offense
description	text	Detailed description of the incident
evidencePath	varchar(255)	File path to uploaded evidence (e.g., image)
createdBy	int(11)	Foreign key linking to users.userID
status	varchar(20)	Case status (e.g., open, closed)

Table 6: Data Dictionary of Table "Disciplinary_Cases"

The disciplinary cases table will record all cases of misconduct that will be reported in the system. It has a primary key, caseID, and foreign key, studentID, which is referred to the Students table. The table will store significant data like date of case, time, type of offense and a brief description of the case. The evidence which supports the evidence is stored in a file path format within evidencepath and createdBy field is used to associate this case to the staff member who reported this case. Status field shows whether the case is open, closed or under review.

The central part of the disciplinary system is this table: through it, a well-organized case tracking will be possible, and the staff and the administration users will be able to deal with the incidents easily. Case handling is transparent and accountable due to evidence and timestamps.

Field Name	Data Type (Size)	Description
historyID	int(11)	Primary key; unique identifier for each action
caseID	int(11)	Foreign key linking to disciplinary_cases.caseID
actionDate	datetime	Date the action was performed
actionType	varchar(50)	Type of action (e.g., update, close)
actorID	int(11)	Foreign key linking to users.userID

Table 7: Data Dictionary of Table "Case_History"

The case history table records all the activities done on disciplinary cases chronologically. Every line in this table is distinctly denoted by historyID and related with a particular case by caseID. ActionDate records the date on which the action was undertaken; actionType records the nature of update that has been undertaken- such as case creation, status change or comment added. The user who performed the action is connected to the actorID and this makes them traceable.

This table also supports the accountability and audit features of the system, such as case development, who made such changes, and at what date and time, which allows the administrators to be consistent in disciplinary actions. It also increases adherence to the policies of data governance and internal review of the system.

6.3.2 Data Flow Diagram (DFD)

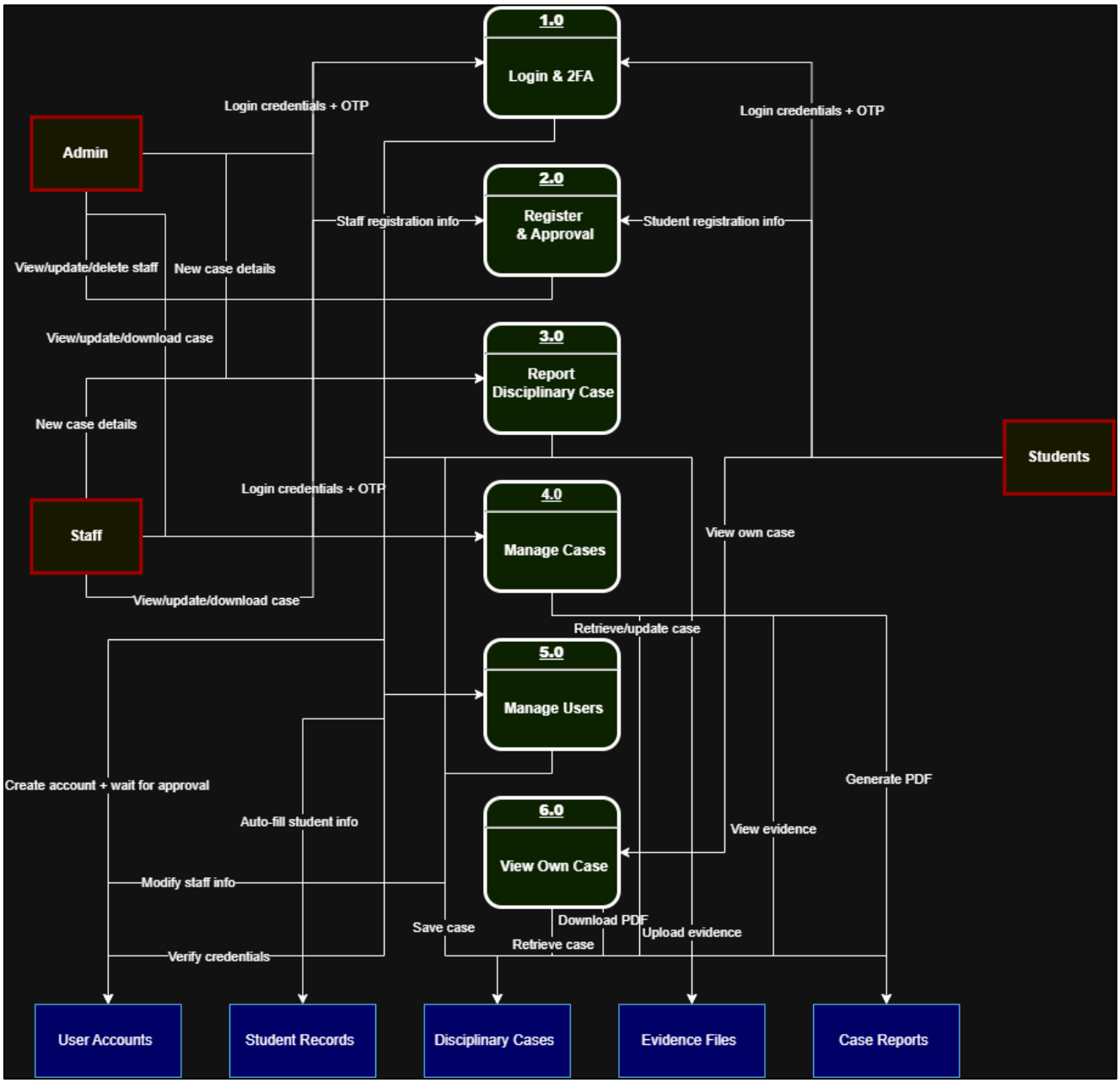


Figure 38: Data Flow Diagram (DFD) for Secure Student Disciplinary Record Management System

The Data Flow Diagram (DFD) of the Secure Student Disciplinary Record Management System represents how data flows between the external entities, fundamental system operations and data stores. This Level 1 DFD reduces the system architecture to 6 key processes: Login and 2FA Verification, Register and Approval, Report Disciplinary Case, Manage Cases, Manage Users and View Own Case.

Granting access to processes is based on permission based on the role of the user. Admins will have full access to all modules such as user additions, and deletions of cases. The staff users have access to the functionality of reporting and dealing with disciplinary cases but will need permission of an admin to carry it out through the system. Learners are only allowed to look and download their disciplinary records.

It is a system where several data stores are incorporated, including User Accounts, Student Records, Disciplinary Cases, Evidence Files, and Case Reports, which maintain properly organized and safe data storage. As an illustration, when a new case is being reported, the information regarding the student is automatically copied to the Student Records store, and the evidence files are uploaded to the Evidence Files store.

The system has security features that allow it to guarantee the confidentiality, integrity, and protection of data against common threats, including password hashing, two-factor authentication (2FA), SQL prepared statements, session hardening, and role-based access control. Such mechanisms in the diagram are echoed by demonstrating secure data streams and limited access routes.

Such a DFD allows a full picture of data flow in the system, which makes the operations secure and role-based and ensures the adherence to the institutional and privacy standards.

6.3.3 System Flow Diagram for Admin

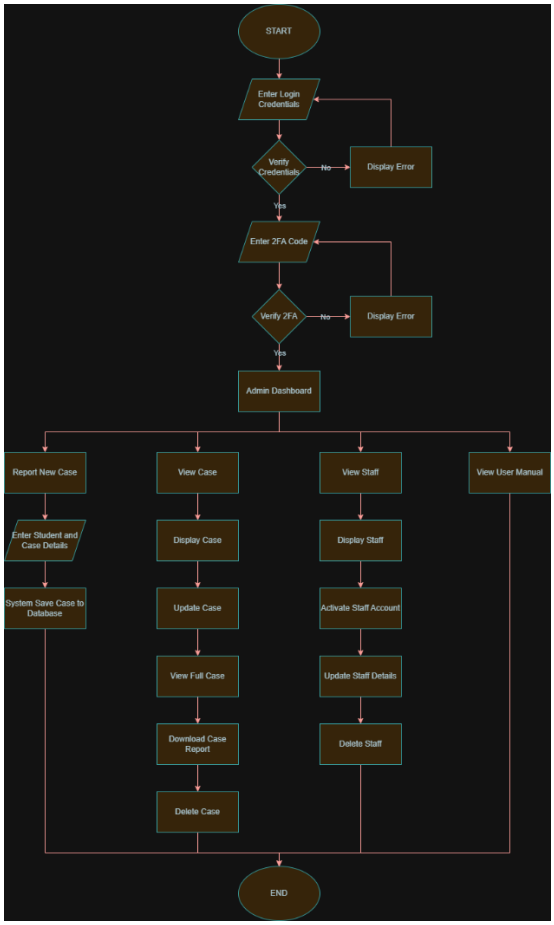


Figure 39: System Flow Diagram – Admin

The Admin system flow begins with a secure login system, which involves the verification of credentials and 2FA, so that only authorized staff can gain access to the administrative dashboard. With a successful authentication, the Admin will be provided with a complex dashboard that will allow him or her to have complete jurisdiction over disciplinary cases and over the management of users. New cases, viewing and updating old records, deletion of cases and downloadable reports to be used either internally or as audit related are all made possible.

Other than case management, the Admin can also manage staff accounts by enabling, updating, or deactivating staff profile. The user manual is also available in the system to aid the user. Every activity being implemented by the Admin is recorded so that actions can be monitored and be held accountable, which is a sign of the dedication of the system towards transparency and integrity of data. This flow is such that the Admin position has a centralized control of all disciplinary functions without going against both PDPA and institutional standards of governance.

6.3.4 System Flow Diagram for Staff

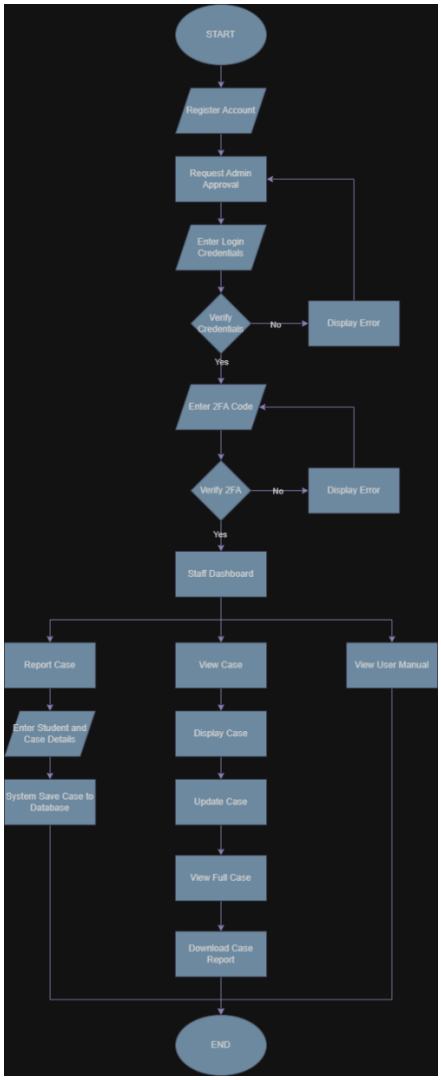


Figure 40: System Flow Diagram – Staff

The Staff system flow begins with the registration of accounts taking place in the Staff system, which proceeds to Admin to validate the accounts to be used by only the recognized personnel. The next step will be to obtain an approval and enable the staff to log in using secure credentials and a 2FA identification process. On a successful log-in, they would be redirected to the Staff Dashboard, and the main functions would be reporting the new disciplinary cases, viewing and updating the current record, and downloading case reports.

It prevents employees working with cases removal and accessing any information beyond his/her mandate and therefore maintains confidentiality and role-based access. The system is also provided with a user manual which will assist the staff adhere to the working procedures. All the actions performed by the staff are documented in the activity log of the system, thereby rendering it auditable and internal review. This flow will allow the staff to handle the disciplinary cases in the most efficient manner without violating data protection and operational limits.

6.3.5 System Flow Diagram for Student

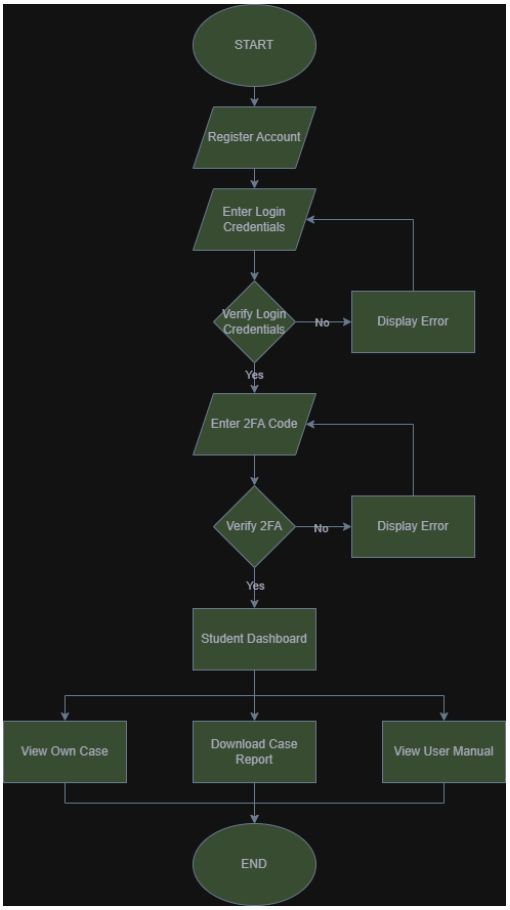


Figure 41: System Flow Diagram – Student

Student system flow is developed in the way that is privacy-and-easy-minded. The student will initially create an account, log in with security, and mark it out with 2FA to get access. Then they are redirected to Student Dashboard, which shows the student only the disciplinary records and this is in line with the PDPA and confidentiality.

It enables students to see their detailed information about their cases on the dashboard and the ability to download their case reports to save it in their personal files and watch a user manual on how to use it. This system is such that students cannot view or edit any information other than the information concerning them- a good example of the principle of least privilege. Such flow contributes to the enhancement of transparency and allows students to be aware of their disciplinary status so that their sensitive data is not violated and access is highly restricted.

6.3.6 Entity Relational Diagram (ERD)

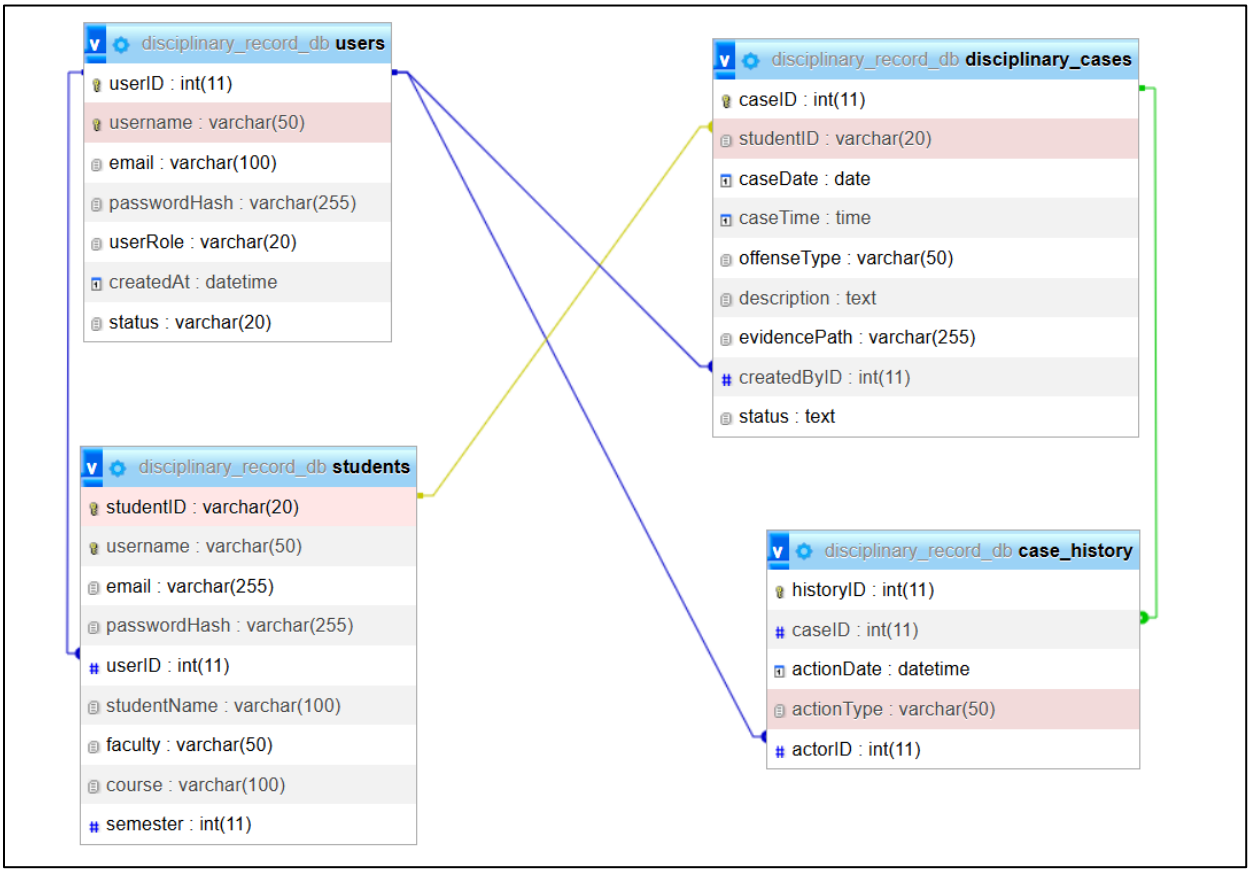


Figure 42: Entity Relationship Diagram (ERD)

The ER diagram of the Secure Student Disciplinary Record Management System establishes the major database design that can facilitate efficient and safe data management. It defines the connection among the significant entities, such as the users, students, disciplinary_cases, and case_history, in order to safely store information in a normalized and relational form. The structure plays a pivotal role in managing both the integrity of data and access control and thus the precision in monitoring all the occurrences of disciplinary measures.

Users table is a central authentication authority that stores the login credentials, roles and fleet timestamps. The student table identifies the students with the user account and gathers personal and academic data concerning the students. Disciplinary_cases table records data on the offence type, evidence, and status of case, which are associated with the corresponding student. The case_history table records all activities done on a case, including updates and determinations as well as the person who did it. These referential integrity and secure role-based access to sensitive data are aided by foreign key constraints between them. The system has a secure, scalable, and compliant data architecture that is supported by the ERD.

6.4 Security System Framework

One of the major considerations in designing the Secure Student Disciplinary Record Management System would be security as data on misconduct among students is sensitive and there would be a legal requirement as stipulated in the Personal Data Protection Act of Malaysia. A design of such a system should aim at ensuring that the disciplinary actions can only be changed, modified or viewed by authorized persons and safeguard the integrity, confidentiality, and availability of the data. The detailed security model is built that is characterized by various levels of protection as well as authentication, authorization, data management, and role management.

This model is structured based on five fundamental security concepts namely Confidentiality, Integrity, Availability, Accountability, and Authentication and Authorization. Further consideration is given to the User Role Management. All of these principles are specifically technicalized, such as password hashing with the support of Bcrypt, role-based access control, Two-Factor Authentication (2FA), input validations, SQL prepared statements, session timeouts, and tracing of case statuses. These factors are used together to ensure the security of the system against different threats including unauthorized access, data breach, and manipulation, and also to make sure that the system is still accessible to the Admins, Staff, and Students.

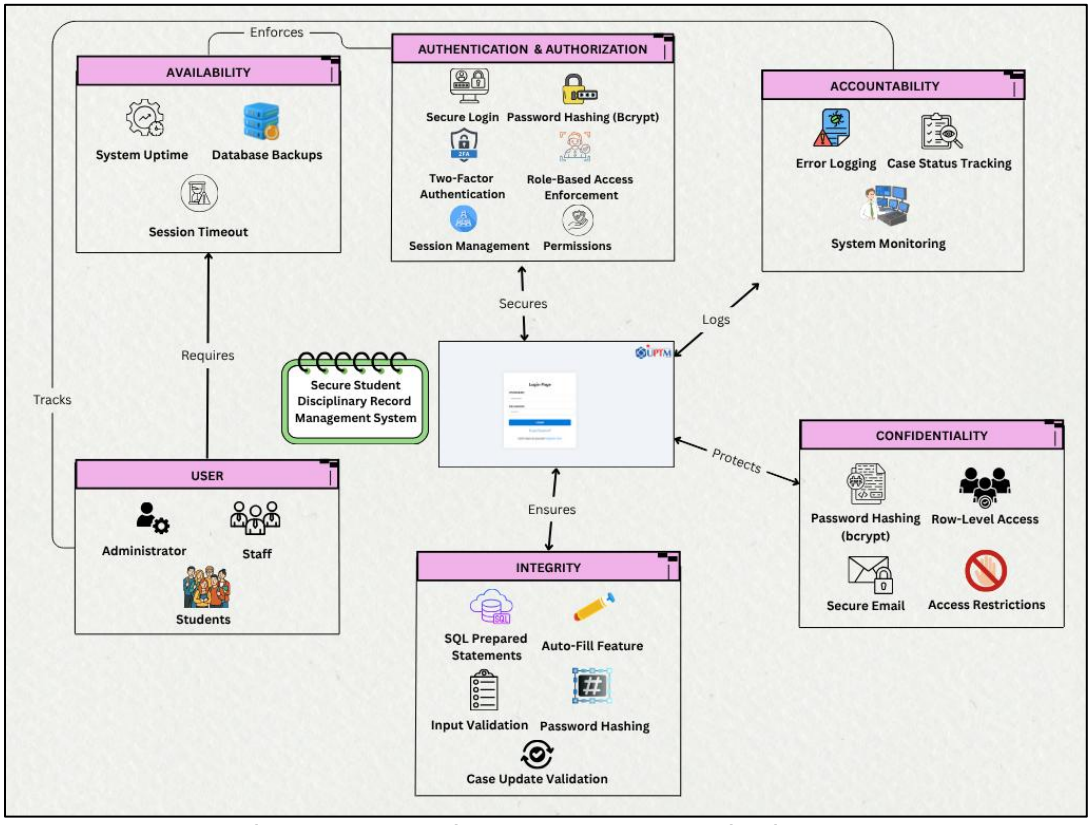


Figure 43: Security System Framework Diagram

Each security domain as demonstrated in this diagram plays a different role in securing the overall system. Authentication and Authorization enforce users to be verified and access control based on their roles, secure login, password hashing with Bcrypt, 2FA, session management, and permission controls. These controls offer defense against unauthorized access and guarantee that every user does not use the entire system as a whole but only that portion of the system that is pertinent to them in their work.

As the access controls are restricted and the data is visible on a row level, confidentiality is ensured in which the student records are to be accessed by the right users. The role-based access control will enable students to access the case of other students whereas staff is limited to do acts of administration. Although encrypted communication and secure email are the best practices, the existing system is based on the internal control of access and management of sensitive data as a means of information protection.

Validity is checked through input validation, SQL prepared statements, and case update validation. The mechanisms help to prevent data tampering, injection attacks and the unintentional corruption of disciplinary records. The system will help to ensure that data stored is accurate and reliable as only valid and authorized changes to the data are allowed.

The session timeouts policy supports availability, and it helps in the strategies of backing up the database. These features will prevent unauthorized access because of idle sessions and guard against the loss of data in the event that the system fails. Although the system does not adopt cloud hosting, it is designed in a manner that can be stable and available in the environment where it will be deployed.

System monitoring, error recording and case tracking facilitate accountability. The system does not fully have audit trails, but the status of an open or closed disciplinary case can be viewed by Admin and Staff, hence, providing some level of transparency. It promotes accountability of actions and responsibility in handling cases in the system.

User Role Management establishes three roles namely Administrator, Staff, and Student. There are varying access levels and duties in each of these positions. The Administrators are in full control of the system, the Staff handle daily operations of the cases and the Students can safely view their disciplinary records. With this, all these elements combined would constitute a sound and adherent security architecture that supports the mission of the system which is to maintain disciplinary records safely and effectively.

6.5 Conclusion

The Secure Student Disciplinary Record Management System has carefully been designed to overcome the fundamental problems that have been seen in the previous chapters, and especially those that concern the keeping of records, access control, and effective tracking of cases. The system has now offered a multi-layered security architecture in which by sensitive disciplinary information is under the protection of string authentication, authorization, input validation, and role-based access control. The design has features that can be customized to access by Admins, Staff and Students- a feature that would fit the workings of the Student Affairs Division and demands of transparency and privacy under PDPA.

The project is now set to enter implementation phase given that its system architecture, database schema and security framework are well defined. The concept of the system modules will be developed in the following chapters and security features will be integrated in the system and the design shall be tested against the real world. In this respect, such development process implies going a step further into a concrete, workable, secure, and user-friendly application that would improve the disciplinary management process of the university.

7 IMPLEMENTATION

7.1 Introduction

This chapter outlines how the safe student disciplinary record management system was put into practice. Some of the areas of discussion are the platform of execution, software tools, hardware tools utilized, system interface, key functions- notably security features and status of system. The system was generated through iterative process, and it began with prototype versions which guaranteed adequate operability, user-friendliness, and security standards. By the time of submission, the system will be fully operational and will be ready to be implemented in Student Affairs Division of UPTM.

Secure Student Disciplinary Record Management System is aimed at keeping the disciplinary records of students safely and keeping confidential information. During the implementation, great attention was given to provide features of high levels of safety, convenient interface, and the ability of the system to work with the back-end. Difficulties that were faced comprised of making sure to have a secure authentication, SQL injection is avoided, and correct session management.

7.2 Execution Platform

7.2.1 Development Platform

Figure 44: Windows 11 Pro (Development Platform)

Windows 11 Pro is the main operating system that will be used when developing and testing the Secure Student Disciplinary Record Management System. This operating system provides a constant and compatible environment in which development tools, database servers, and testing of the system can be performed in numerous browsers. The OS makes sure that the software development process is hassle-free and system dependencies such as the .NET frameworks can be run on the system with no compatibility problems.

7.2.2 IDE for Backend & Frontend Development

Figure 45: Visual Studio Code IDE

VS code is the main IDE in the development of the backend and frontend components of the Secure Student Disciplinary Record Management System. The IDE works with PHP that is required to develop the back-end and with HTML, CSS and JavaScript to create the front-end interface. VS Code offers the necessary functionality that simplifies the process of coding such as syntax highlighting, IntelliSense, auto-formatting, and built-in terminal. In addition to these, there are extensions like PHP IntelliSense, Live Server and MySQL integration that eventually add value to this development experience by easing debugging process, enabling database connection and testing interfaces akin to real time.

7.2.3 Data Storage and Management

Figure 46: MySQL Database Management

MySQL Database is a well-known and global used database management system in which I think has grown in recent years. MySQL is the relational database management system (RDBMS) in which sensitive student disciplinary records will be stored in a secure storage. It administers user accounts, hashed passwords using the bcrypt hash, and system logs. Data integrity and SQL injection attacks are safeguarded by the fact that prepared statements are used in MySQL. Visual Studio Code is used to interact with the database with the backend logic when the system is run.

7.3 Implementation Tools

This part will describe the software and hardware resources that were used in the development and implementation of the Secure Student Disciplinary Record Management System. The choice of tools was made wisely to support the efficient development, testing and deployment of the system taking into consideration system security and reliability.

7.3.1 Software

7.3.1.1 Operating System (Windows 11 Pro)

Figure 47: Windows 11 Pro

The primary software environment used in the development of the system is Windows 11 Pro. It can be compatible with such relevant development tools as Visual Studio Code, MySQL, and XAMPP. The OS is compatible with the easy installation of local servers, command line interfaces and PHP extensions needed in the back-end development. It is stable and has a broad range of development utilities that will guarantee a smooth flow during the implementation phase.

7.3.1.2 Database Management System

Figure 48: MySQL Database Management

MySQL is a relational database management system that is used to save all the information in the system in a secure manner. It deals with records about student disciplinary action, user accounts, session logs, and all other important information. Although MySQL has prepared statements that avoid SQL injection attacks thus maintaining integrity and security of data, it directly interacts with the PHP back end to fetch, insert, update and delete records dynamically. It forms a key element towards effective control of the data contained in the system.

7.3.1.3 Programming Language

Figure 49: PHP

PHP is the core language for developing the system's backend. It is used to process user input, manage sessions, perform form validation, and interact with the MySQL database. PHP was selected because it works well with MySQL and is popularly employed in the development of secure web-based applications. For the frontend, HTML structures each page, while CSS controls the design and layout. JavaScript is used to add interactivity to things like form validation, alerts, and smooth navigation. This suite of languages enables the system to be powerful and yet clean and modern-looking for the staff of the Student Affairs Division.

7.3.1.4 Web Server (Apache via XAMPP)

Figure 50: Apache via XAMPP Web Server

Apache, via XAMPP, provides the local web server environment where the PHP-based system is hosted during development. It enables the execution of the backend scripts locally-the actual way the system will behave in a production environment. The web server routes, manages sessions, and communicates between PHP scripts and the MySQL database. Apache allows for easy testing of the authentication flow, disciplinary record management modules, and security features.

7.3.1.5 Integrated Development Environment (Visual Studio Code)

Figure 51: Visual Studio Code IDE

The implementation of the system used Visual Studio Code as the primary code editor. Since it is lightweight, extensions for PHP development, syntax highlighting, and Git integration proved apt for writing clean, maintainable code. VS Code was used in organizing backend and frontend files, testing PHP scripts, and debugging efficiently. The integrated terminal even allowed direct execution of commands, like running Composer installations or testing PHP configurations, and thus improved the workflow throughout.

7.3.1.6 Web Browser (Google Chrome)

Figure 52: Google Chrome Browser

Google Chrome was the main browser used for interface testing and system validation, from HTML/CSS inspection to JavaScript errors and responsive layout tests. Chrome was also used to test secured pages, login sessions, role-based access controls, and 2FA verification flows. This makes it quite important in the validation of functionality and usability before deployment.

7.3.2. Hardware

Figure 53: MSI Thin GF63 Development Machine

The primary hardware components that are going to be used in the implementation and testing of the Secure Student Disciplinary Record Management System are an MSI Thin GF63 10UC-432X 15.6" FHD Gaming Laptop. The laptop has enough RAM and processing unit to support several development tools operating simultaneously including Visual Studio Code, MySQL, Apache server (using XAMPP) and web browsers to test. The Intel-based CPU has an inbuilt graphic card that is smooth in execution of the programs, database setup and testing of the system. Quick SSD storage enhances handling of files as well as reduces the time taken in loading one module of the system to another. In this way, MSI Thin GF63 becomes a solid and effective workstation during the whole implementation process, which can support all the features of developing, debugging, and testing the project locally.

Specification	Description
Development Machine	MSI Thin GF63 10UC-432X
Processor	Intel® Core™ i5-10500H (2.50 GHz)
RAM	8GB GDDR6
Storage	512GB HD
Display	15.6" Full HD
Network	Stable Wi-Fi internet connection

Table 8: Hardware Specification

7.4 System Interface

The Secure Student Disciplinary Record Management System has an Admin, Staff and Student interface. This system is designed in such a way that it has an easy to use interface, which is user friendly and has security so that users can use it and ensure that the sensitive information is safe. The main functions are login, 2FA Verification, Dashboards, Disciplinary Case Report, User Management, Report Download, and User Manual Consultation. The system will be designed to perform secure and reliable operations by designing workflows that are input-validated, use prepared statements, and have a role-based access control. Each of the modules will be presented with screenshots to show the real interface of the system.

7.4.1 Interface for Each Module

Admin Interface

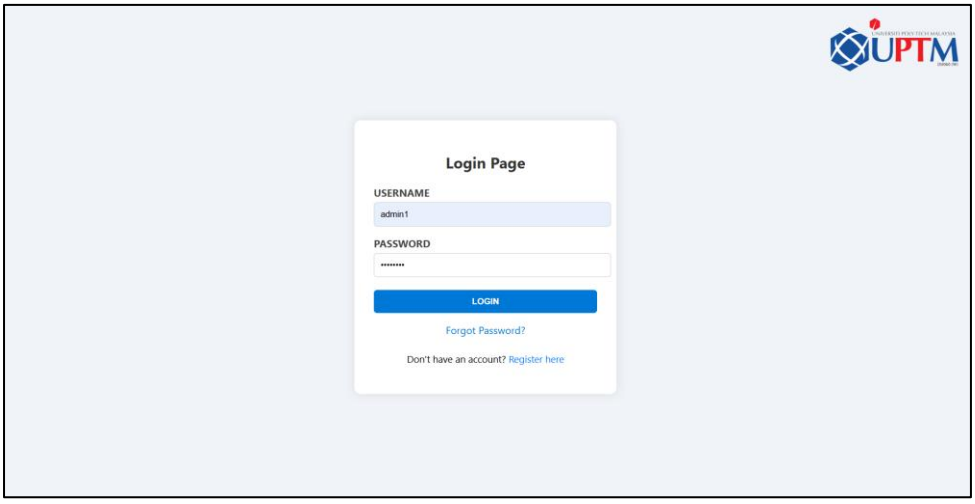


Figure 54: Admin Login Page

The administrator logs in using his/her registered credentials. Input validation inhibits a blank or invalid input and invalid credentials are processed. On successful log in, a secure session is initiated in order to avoid unauthorized access.

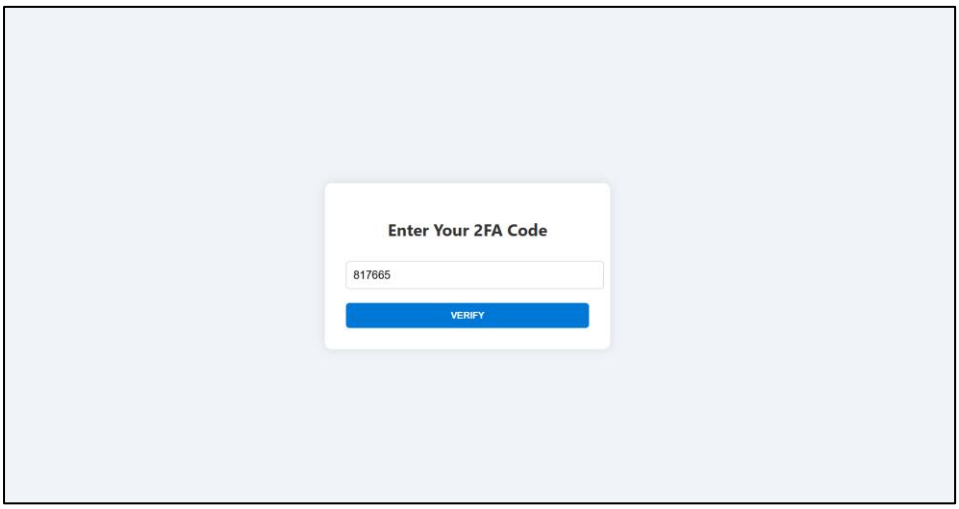


Figure 55: Admin 2FA Verification

After a successful login, the admins are required to key in the OTP that would be forwarded to their email. This gives an added avenue of protection against account theft. The interface is well designed to teach the user how to key in the OTP; it also checks whether the code has expired or entered the wrong code.

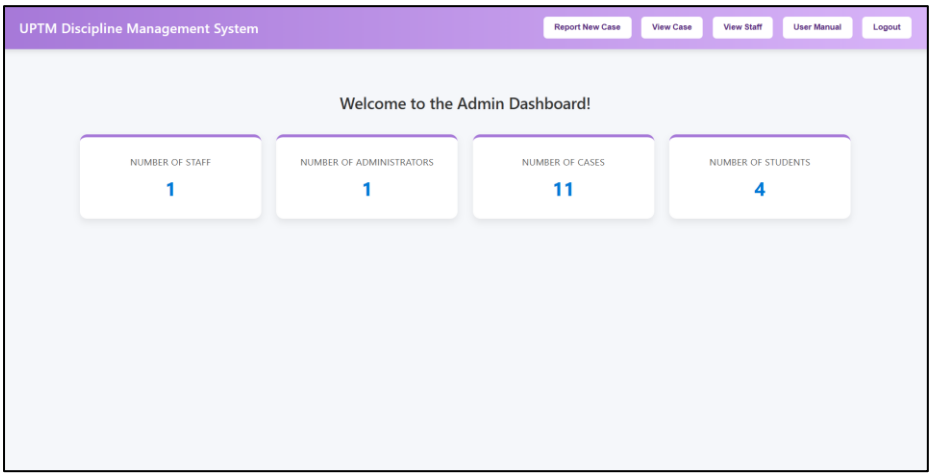


Figure 56: Admin Dashboard

The dashboard gives a summary of the total staff, administrators, number of cases, and the number of students. Quick links to all system modules for navigation allow admins to perform their tasks efficiently. Security is enforced by restricting access based on user roles.

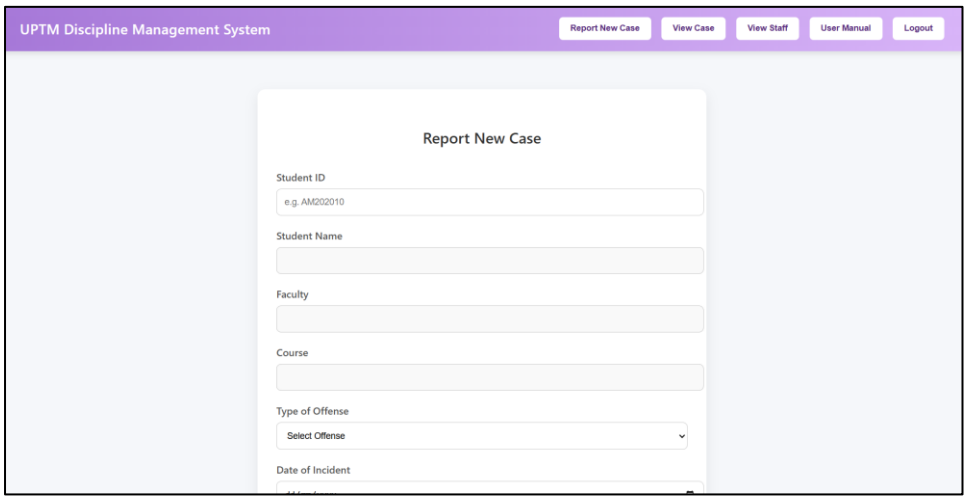


Figure 57: Admin Report New Case

The admin can report new disciplinary cases by filling in student information. An auto-fill functionality is in place by entering a Student ID and it shall automatically fill up the fields of Student Name, Faculty, and Course. Admins can choose the kind of offence-inappropriate attire, disruptive behaviour, sticker vehicle, hairstyle, among others. Other than those, are date, time, provide a description, and can upload supporting evidence in images or PDF. This interface is validated, preventing incomplete submissions from taking place, and utilizes prepared statements to securely insert data into the database.

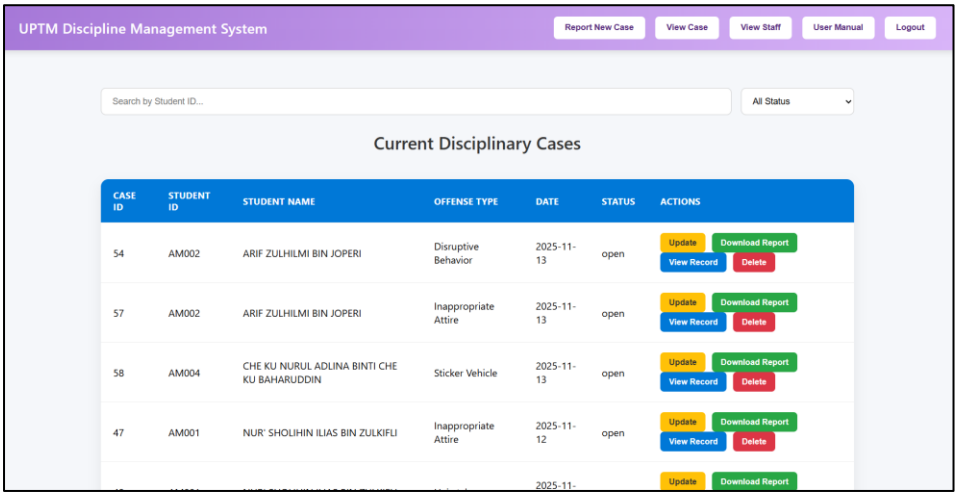


Figure 58: Admin View Cases

This page shows, in tabular form, all current disciplinary cases, including Case ID, Student ID, Student Name, Offense Type, Date, Status, and Actions. Actions include updating cases, downloading PDF reports, showing full records, or deleting cases. All modifications are tracked to maintain integrity and security of the system.

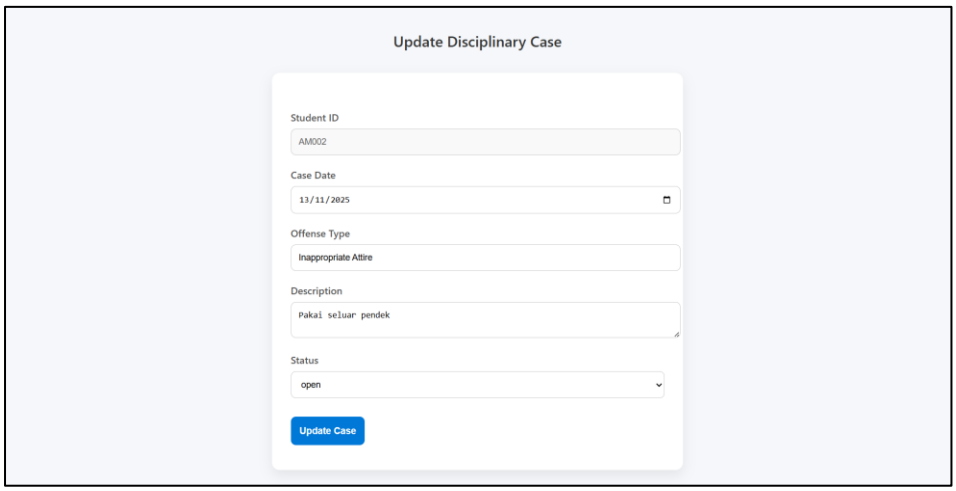


Figure 59: Admin Update Case

When clicked on Update, the admin is redirected to a different page where they can update the date of case, type of offense, description and status (open or closed) depending on its activities. The validation of input is also done to avoid cases where a field is left blank and the desired changes are safely done to the database using prepared statements.

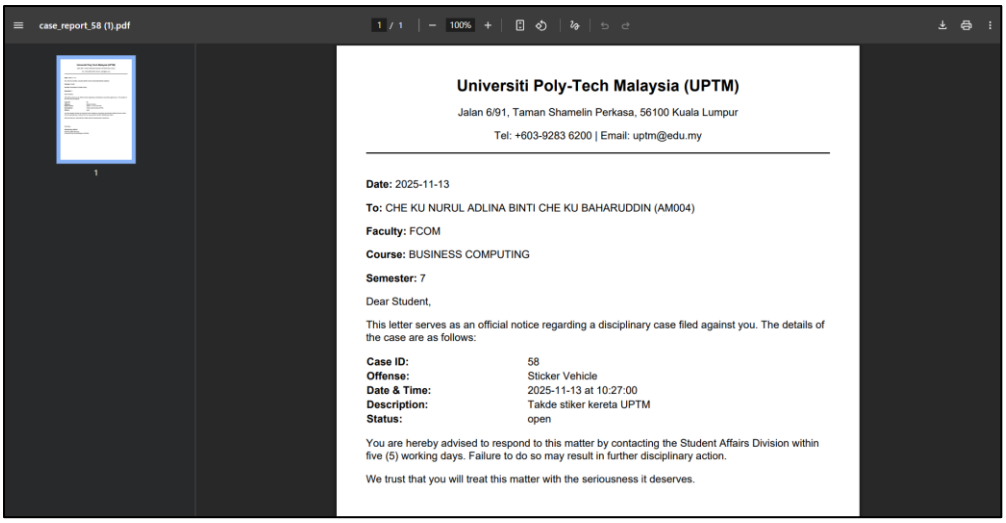


Figure 60: Admin PDF Report Download

By clicking on the Download Report, an official PDF with the information about the students, case ID, type of offense, date/time, description, and case status will be created. It provides a clear preview and the Admin is allowed to save or print the document to use as an official.

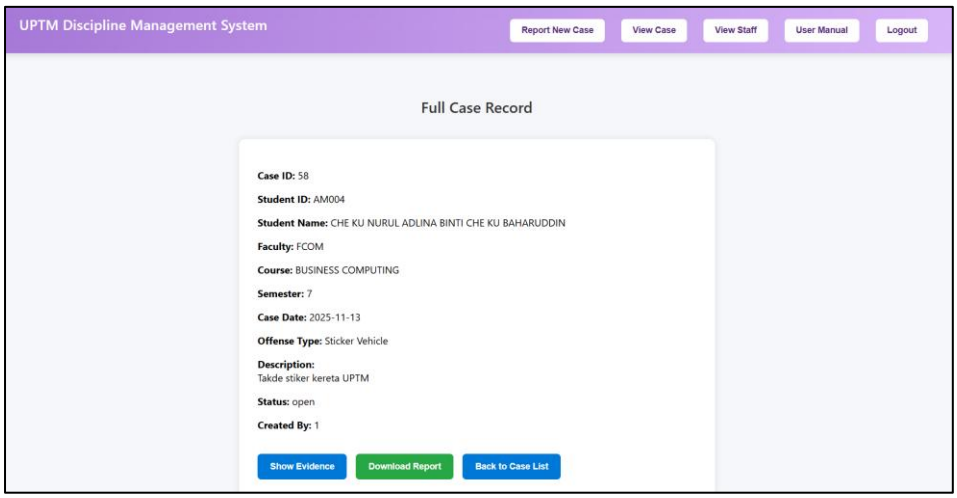


Figure 61: Admin Full Case Record

View Full Case Record option opens to a page where all the information of the student and case is displayed and all of the evidences are uploaded. Here, admins also have access to the complete report of the case in PDF format. This separation makes sure that sensitive information is only accessed when it is required and maintains a sense of direction in its navigation.

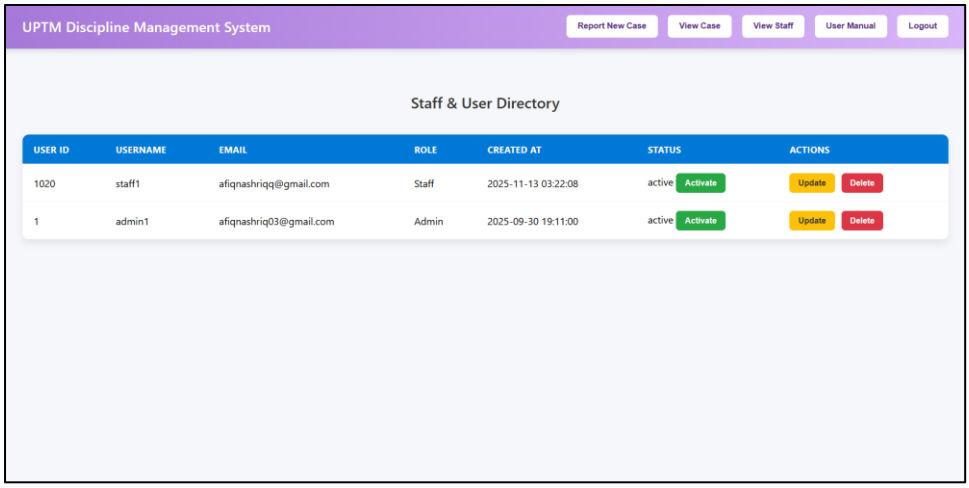


Figure 62: Staff Management Table

The administrator is able to handle personnel accounts in a tabular format with User ID, Username, Email, Role, Created At, Status, and Actions. Admins have a chance to activate staff account, modify the entries, or remove users. Access control will make sure that only admins will be able to do it.

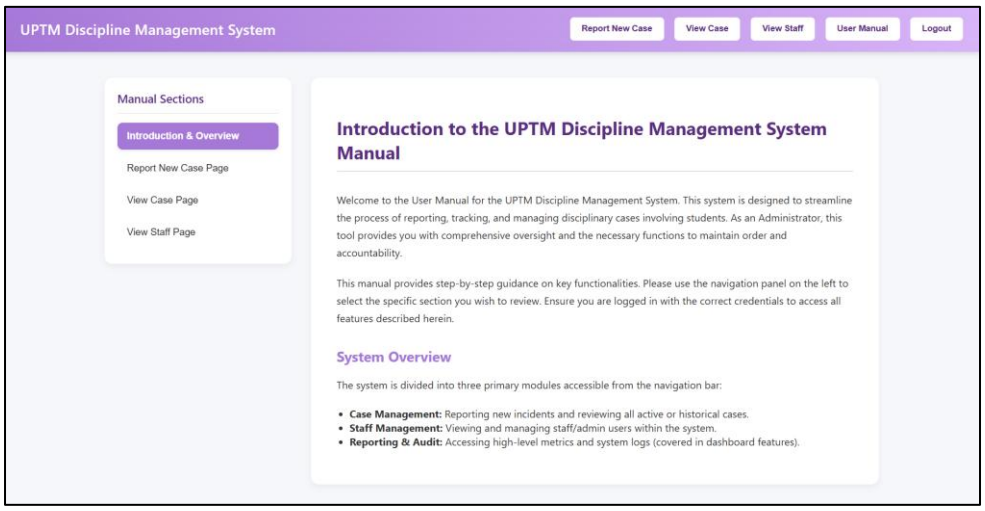


Figure 63: Admin User Manual

This guide is used to give instructions on the use of the system, reporting of cases and maintenance of security standards ensuring that the admins are aware of every process.

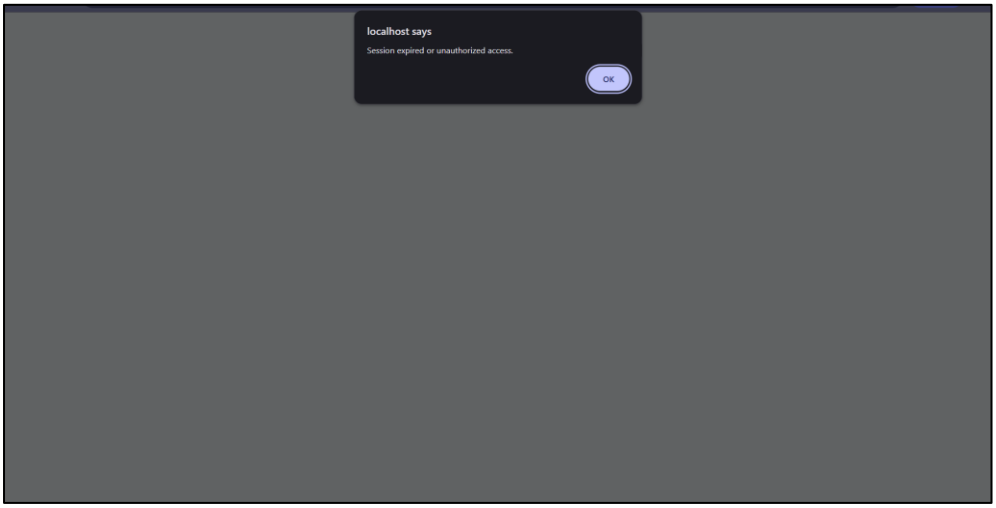


Figure 64: Admin Logout

Sessions are also ended on the logout page and session data is cleared to prevent hijacking; therefore, indicating that the logout was successful. And in case any unauthorized access attempts to turn back to the admin page such attempt will not be fruitful as the session has been expired.

Staff Interface

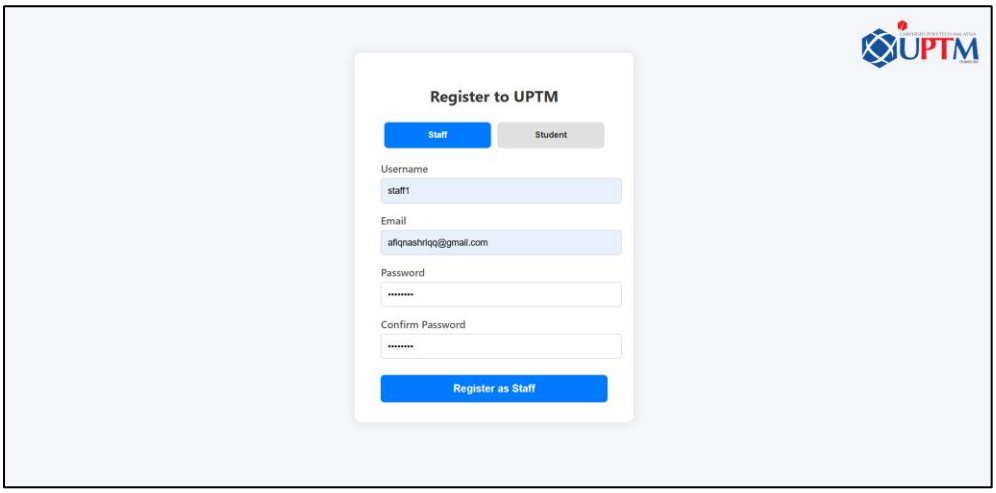


Figure 65: Staff Registration Page

Staff users are allowed to register with provision of the following information: Username, Email and Password. Input checking helps to make sure that fields are properly filled and that they are in accordance with the requirements of the system. When the registration form is submitted, an account is kept in inactive state until an account is approved by an account administrator.

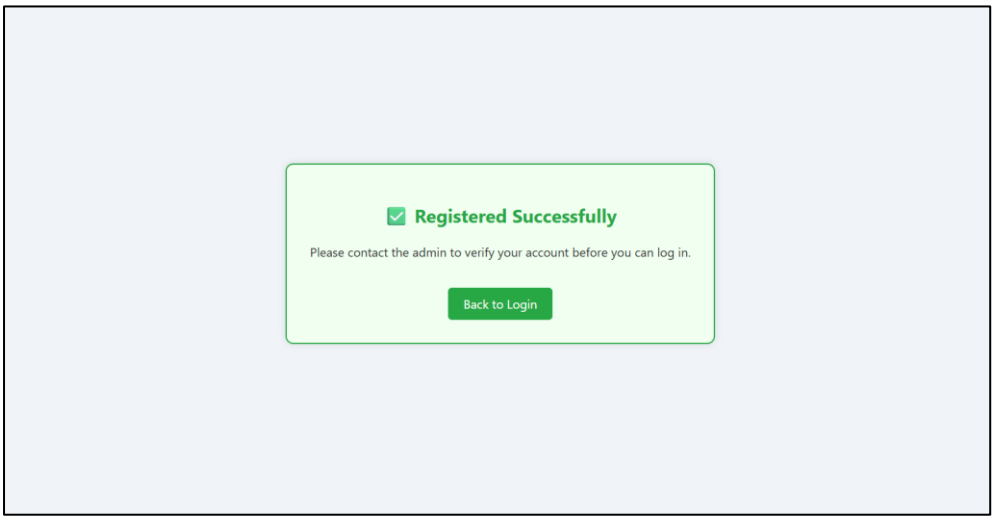


Figure 66: Staff Registration Success Page

Once the registration is successful, the staff will be redirected to a confirmation page with the message: “Registered Successfully. Please contact the admin to verify your account before you can log in”. This page will advise the employees that their account is awaiting approval by the administration. They are not allowed to logins until the admin makes their account active, which is to verify the account and provide the security of the system.

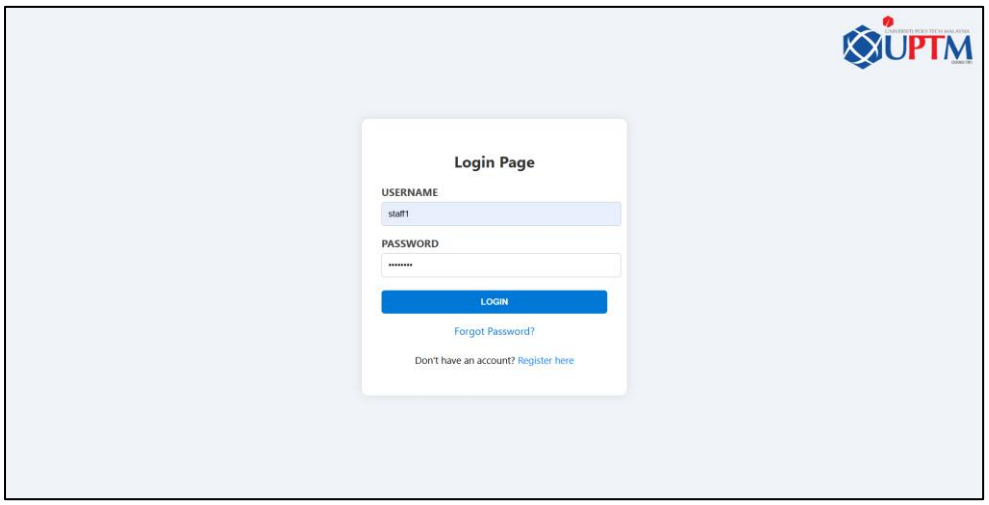


Figure 67: Staff Login Page

Only after the admin verifies his/her account, the staff can log in using the provided credentials. Input validation is performed where only registered and verified users can access the system. After successful login, a secure session is initiated.

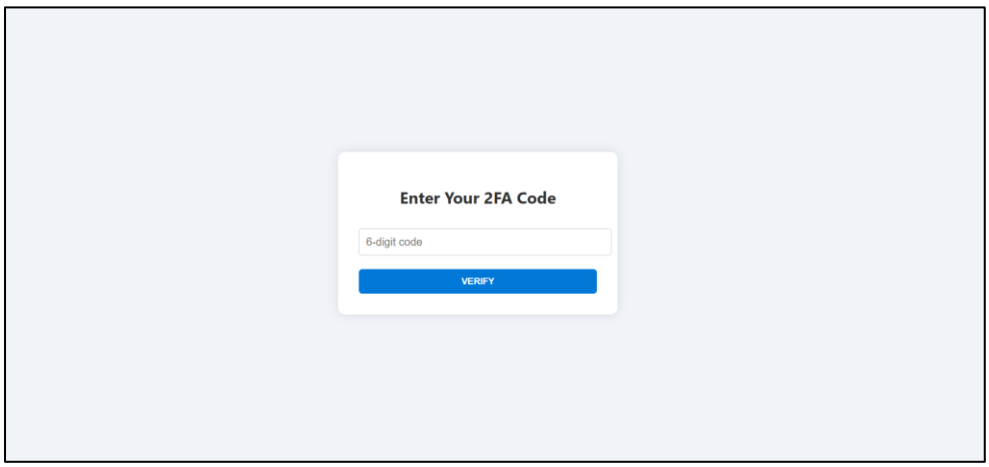


Figure 68: Staff 2FA Verification

After logging in, staff have to enter a One-Time Password that is sent to their email. This further ensures that only authorized users gain access to the dashboard and these accounts are safe from unauthorized access.

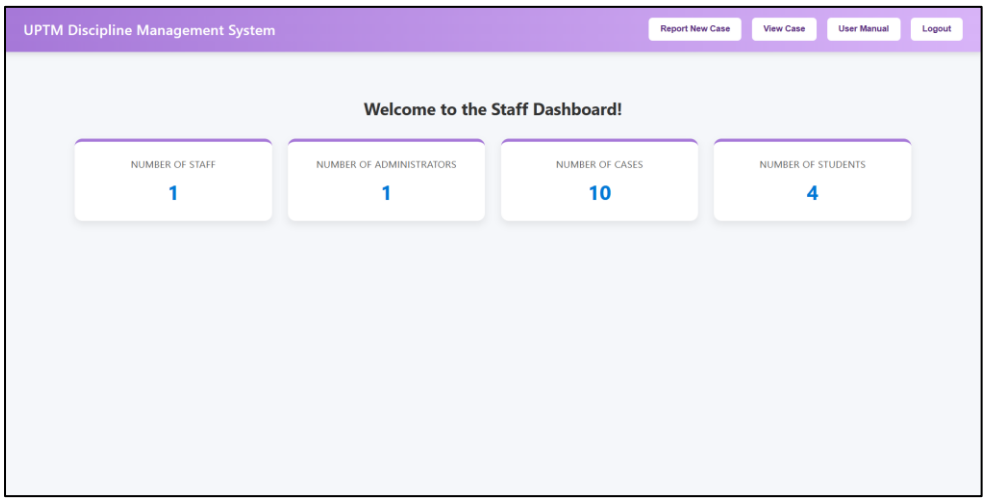


Figure 69: Staff Dashboard

The dashboard gives an overview of tasks and system modules that one can access. It contains links to Report New Case, View Cases, User Manual, and Logout. It also displays the total of staffs, cases, admins, and students. In this way, it acts as a kind of dashboard with vital information about the system. Due to the role-based restriction, some of the modules are not accessible for staff, such as deleting cases or managing staff accounts.

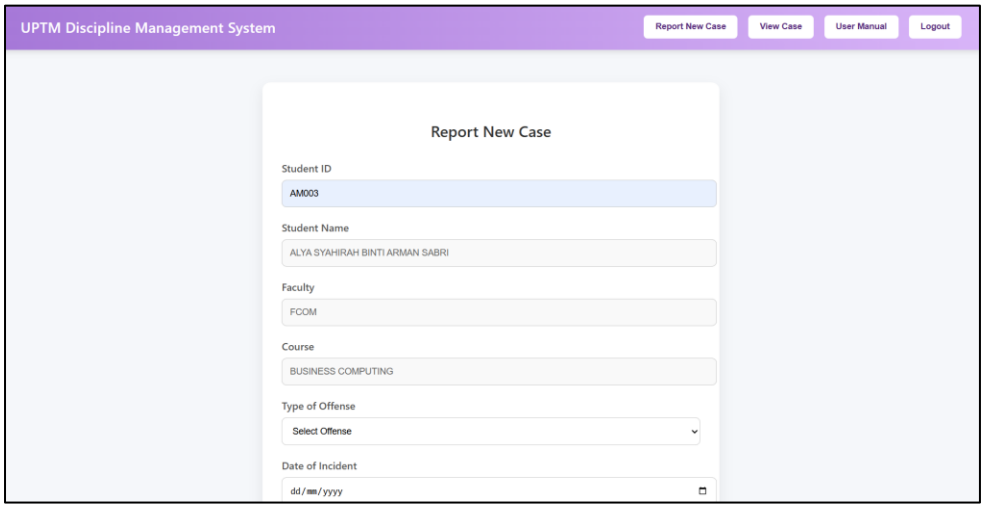


Figure 70: Staff Report New Case

With this module, staff can report new disciplinary cases in a simple, secure manner. By typing the Student ID, the system immediately auto-fills the student's name, faculty, and course to economize time and reduce errors. Staff then select the offense type, provide the date and time of the incident, add descriptions, and attach supporting evidence such as images or PDFs. Inputs are validated for correctness and saved using prepared statements for security, with staff disallowed from deleting or changing cases they did not report, ensuring access control.

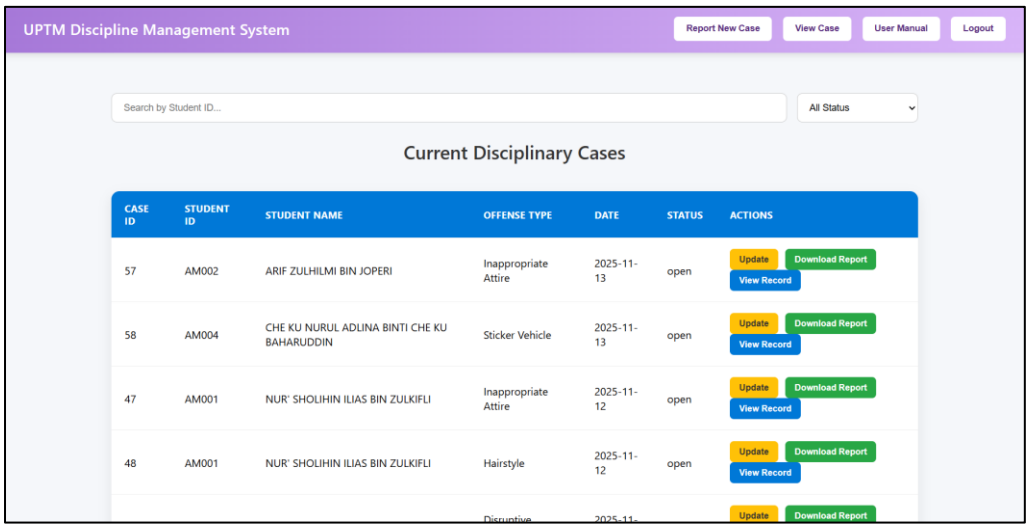


Figure 71: Staff View Cases Table

The page above illustrates all disciplinary cases that the staff is permitted to handle. It contains columns: Case ID, Student ID, Student Name, Offense Type, Date, Status and Actions. Staff can view in a glance the details of the case on each row. Actions column enables them to update a case, or download reports or see complete records. This is a role-based access control given that the staff members cannot delete cases.

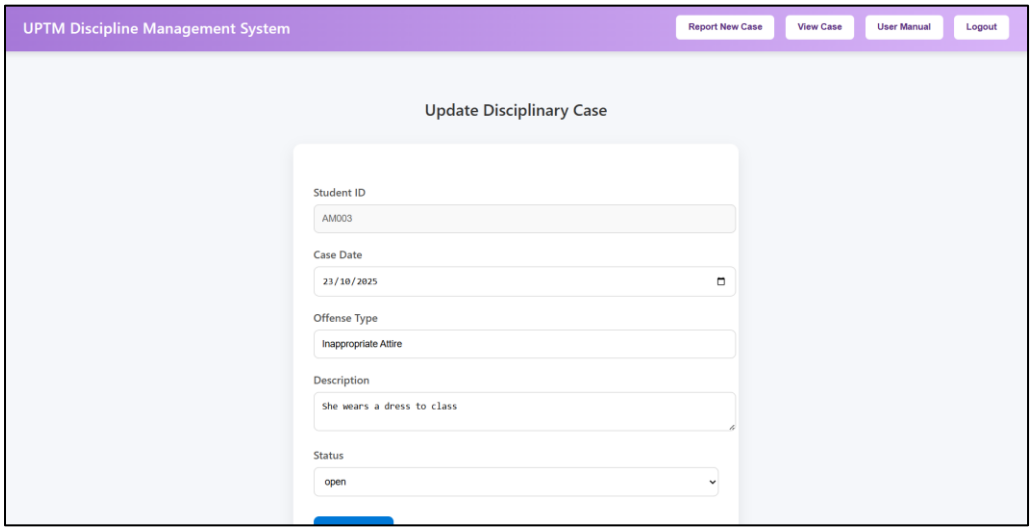


Figure 72: Staff Update Case

After clicking the Update button, the staff will be redirected to the page where they will be able to change the date, a type of offense, the description, and status (open or closed). Status indicates whether the case is still pending or when it is settled. Input validation is applied by use of prepared statements that ensure the updates are safely stored in the database. No cases can be deleted by staff and this further strengthens the control of system security and access.

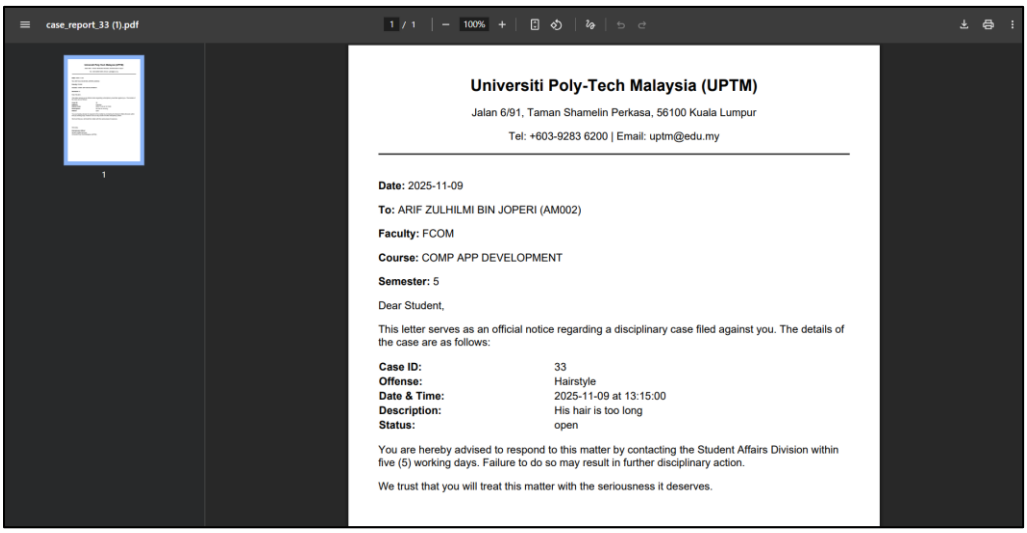


Figure 73: Staff PDF Report Download

After clicking Download Report, an official PDF will be created with all the data about cases, such as student data, case ID, type of offense, date/time, description, and status. It gives the staff the chance to ensure that they maintain proper documentation to be used in an official manner concerning the disciplinary case, and the system ensures that the information will be handled in a secure manner.

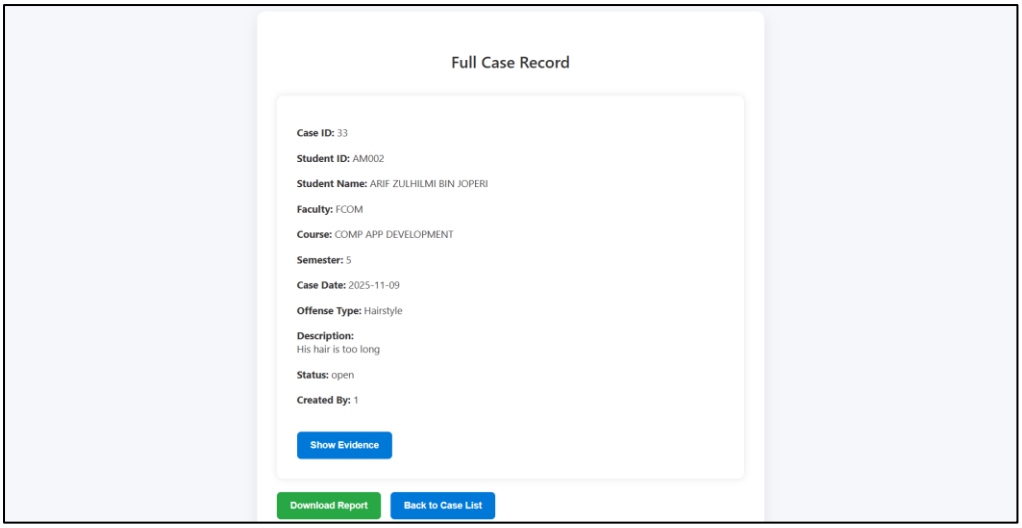


Figure 74: Staff Full Case Record

View Full Case Record option is an option that opens a detailed page on which the staff members can see all data related to the discipline case and files of evidence uploaded in image or PDF format. Moreover, the staff may download the complete report in PDF format, and it is also prohibited to delete the cases of other staff members to adhere to the principle of strict role-based access control to secure access to sensitive data.

Student Interface

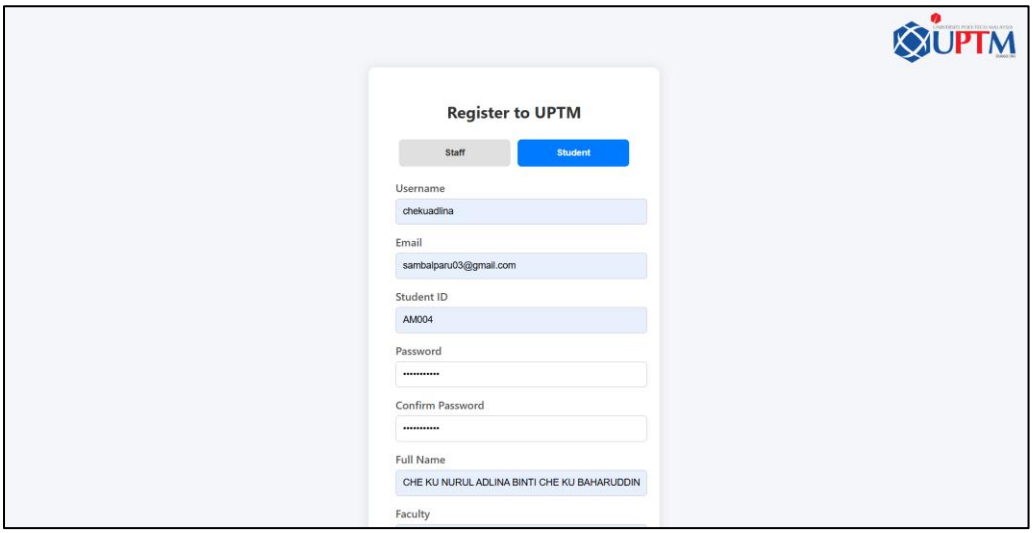


Figure 75: Student Registration Page

Students register generating their username, email, student ID, password, full name, faculty, course, and semester. Input checks verify all the fields that were entered and the password satisfies security measures. This account becomes active at once after the registration.

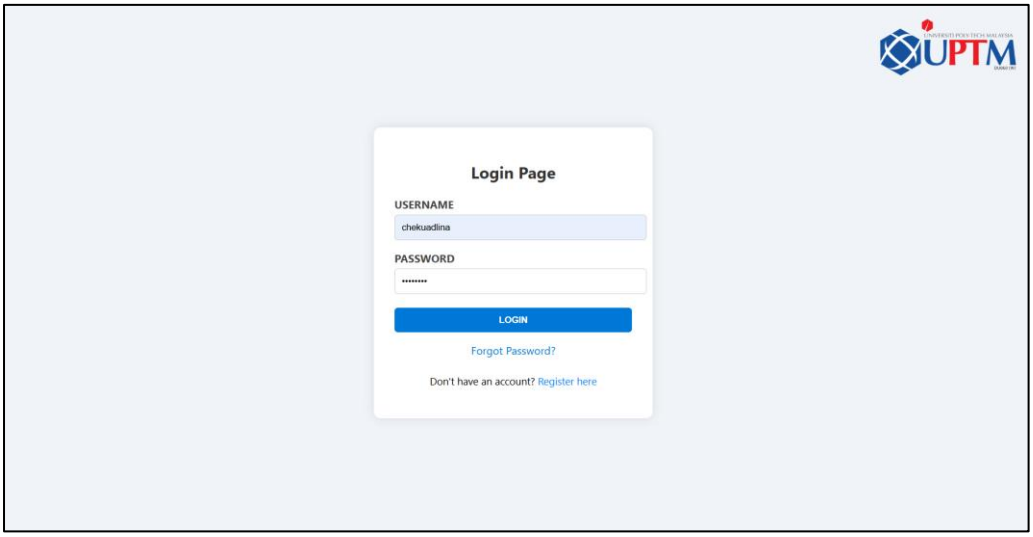


Figure 76: Student Login Page

Students log in with the credentials they registered; the input validation does not allow empty or incorrectly filled-in fields. A secure session is created upon successful login.

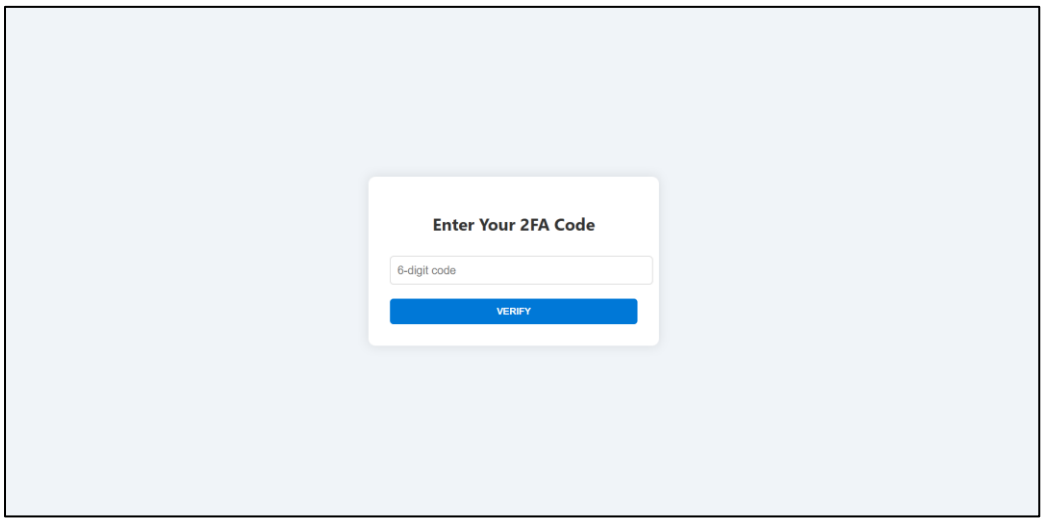


Figure 77: Student 2FA Verification

The student then has to enter an OTP that will be sent to his or her registered email address. This helps the system ensure that the user is authorized to access his or her own disciplinary case information. An error message displays when OTP entered is invalid or expired; a correct OTP redirects the student to the dashboard.

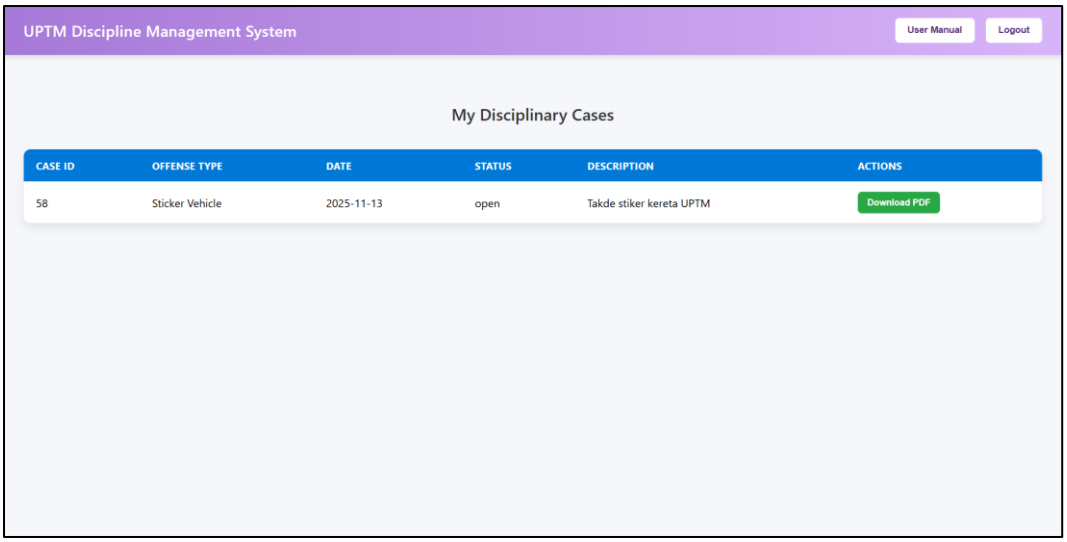


Figure 78: Student Home Page

The Student page gives students a clear overview of their disciplinary cases. The navigation links include Download PDF Report, User Manual, and Logout. Students can access information of their own cases only. The columns include Case ID, Offense Type, Date, Status, and Actions. A student is not permitted to update or delete any cases.

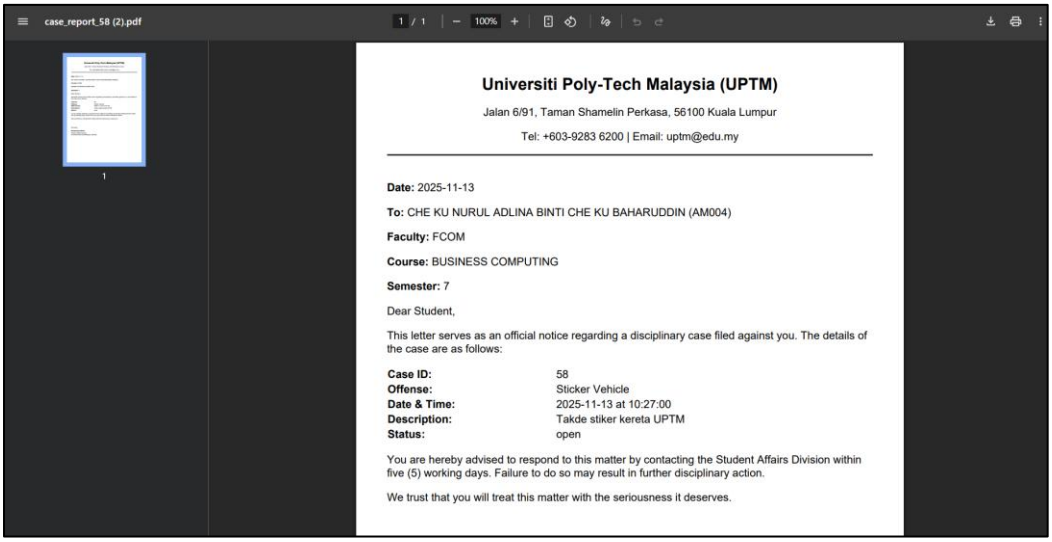


Figure 79: Student PDF Report Download

The students can also download official PDFs of their disciplinary cases that contain all the information pertinent to that case, including student details, case number, the type of offense, date/time, description, and status.

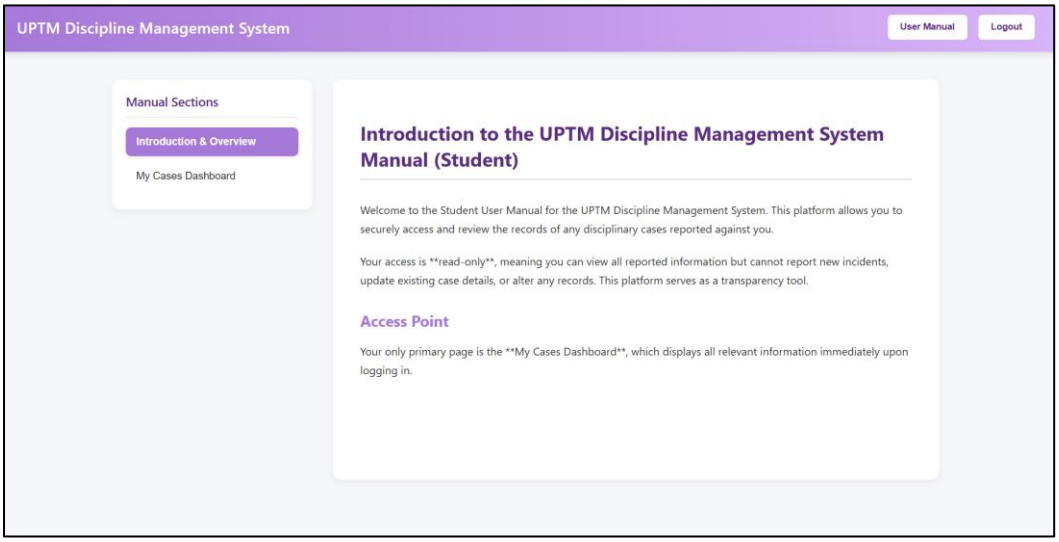


Figure 80: Student User Manual

The manual guides the students on the system, case viewing, report downloading, and proper management of their accounts among others. This also involves the description of security measures including 2FA, session time out and secure log out.

Forgot Password Module

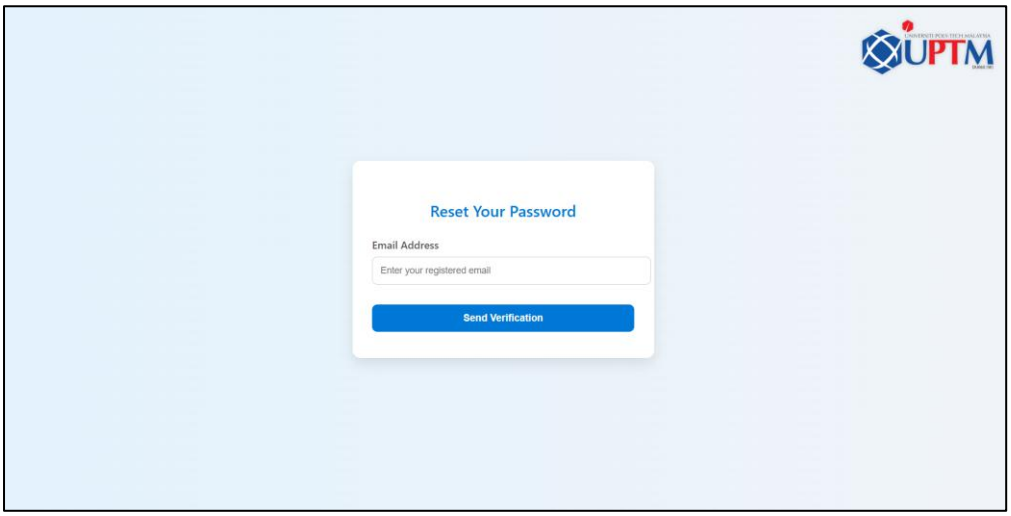


Figure 81: Forgot Password – Enter Email

Email address typed by user: This is the email address that is related with their account. Input validation will also hold back until the email is in the system and no unauthorized attempts to reset the password would be allowed in an account that does not exist.

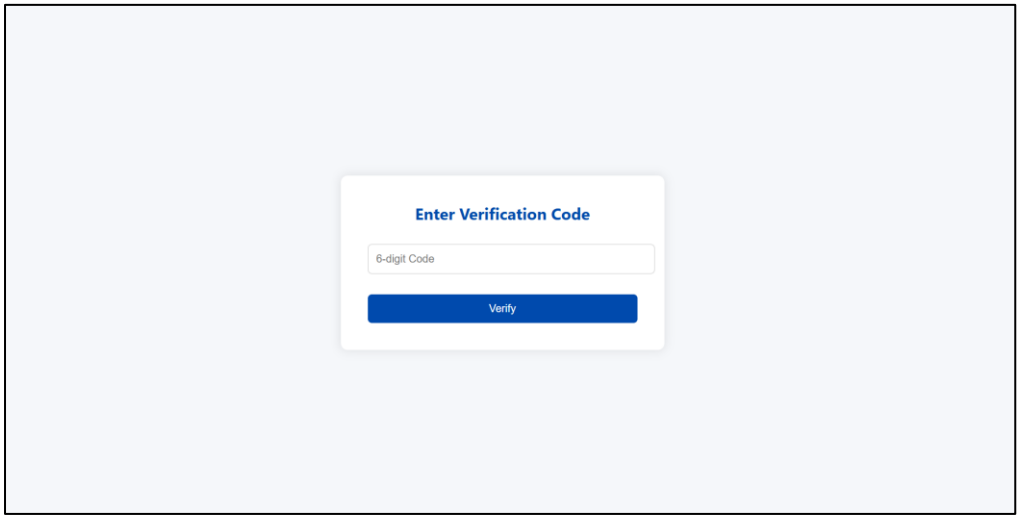


Figure 82: Forgot Password – Enter Verification Code

Then the OTP will be dispatched to the registered e-mail address once the email has been submitted. This code must be entered by the user to confirm his or her identity; the incorrect or out of date code will show an error and the unauthorized access will be prevented. This will ensure that the owner of the account is the only person to reset the password.

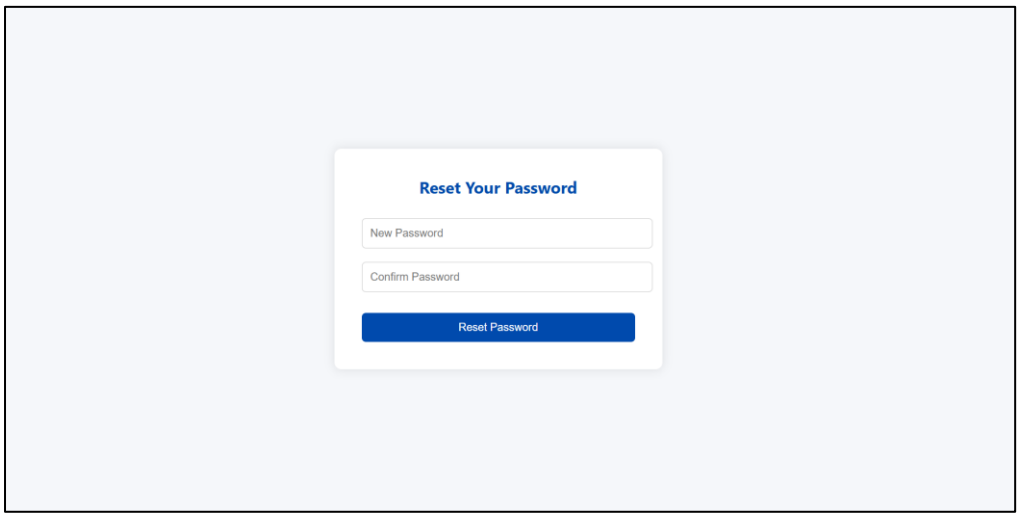


Figure 83: Forgot Password – Enter New Password

When they verify the correctness of the verification code, they are asked to enter a new password. The password rules (e.g., minimum password length, the presence of special characters, etc.) are applied, and the result is hashed securely using bcrypt and then stored in the database. This guarantees that there is total security over user credentials.

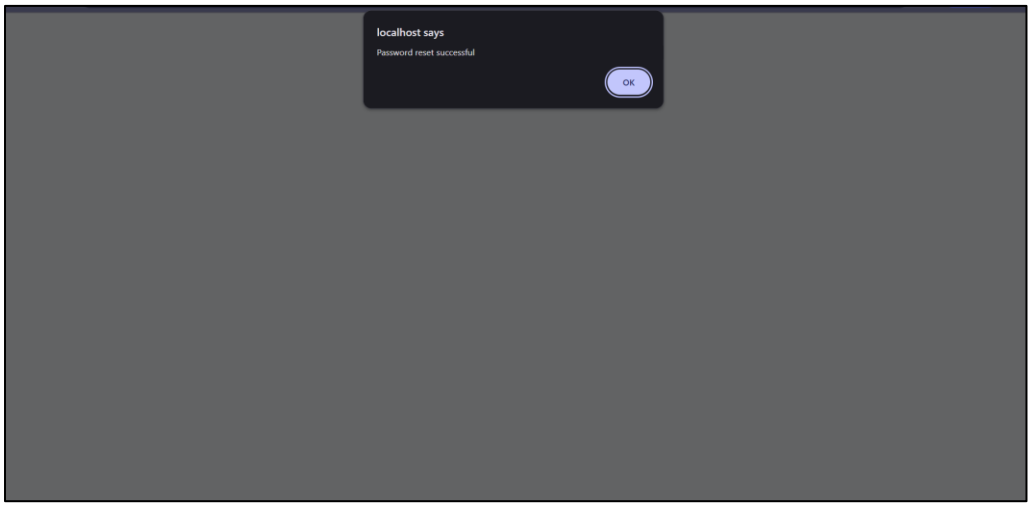


Figure 84: Forgot Password – Reset Successful

When the user manages to create a new password successfully, he/she is redirected to a confirmation page with: "Password Reset Successful" written. This will empty the session and the users are free to log in at any time. This is also to make sure that they do the appropriate clean-up of the sessions as well as secure manipulation of the sensitive account modifications.

7.5 Significant Functions

Security has been one of the priorities used in developing the Secure Student Disciplinary Record Management System. Since the system is dealing with sensitive student and staff information- both personal and disciplinary information- various important functionality has been implemented to maintain the confidentiality, integrity and appropriate access of the data in the system. They are some significant functionalities, which are discussed further in the following sections, as well as code snippets and explanation.

1. Password Hashing (Data Confidentiality)

One of the biggest security features in this system is password hashing. It does not store plain text passwords instead, it uses the password-hash () function provided by PHP to create a secure hash of password of the user and stores it in the database. This implies that even in case such database is compromised, the attackers cannot read the existing passwords since the hashes are stored instead and hence users will not be stolen their credentials.

```
 $passwordHash = password_hash($password, PASSWORD_DEFAULT);
$insertQuery = "INSERT INTO users (username, email, passwordHash, userRole, createdAt,
status)
                    VALUES (?, ?, ?, ?, ?, ?)";
    $stmt = $conn->prepare($insertQuery);
    $stmt->bind_param("ssssss", $username, $email, $passwordHash, $userRole, $createdAt,
$status);
 $stmt->execute();
```

Prepared statements along with hashing will provide security to the system to work with user credentials and also reduce the possibility of SQL injection. Password hashing is also able to give an upgrade to an improved algorithm in the future without compromising the stored passwords.

2. Two-Factor Authentication (Account Protection)

Password security can be enhanced by two-factor authentication. When the user enters correct credentials, it will send a 6-digit verification code to his/her registered email through PHPMailer one time. To do the login they have to fill this code. This aids in preventing unauthorized access even in the event that an individual has stolen a password.

```
$mail = new PHPMailer(true);

try {
  // ☑ SMTP configuration
  $mail->isSMTP();
  $mail->Host = 'smtp.gmail.com';
  $mail->SMTPAuth = true;
  $mail->Username = 'afiqnashriq03@gmail.com';       // Your Gmail
  $mail->Password = 'app_password';        // Your NEW App Password
  $mail->SMTPSecure = 'tls';
  $mail->Port = 587;

  // ☑ Sender and recipient
  $mail->setFrom('afiqnashriq03@gmail.com', 'UPTM Disciplinary System');
  $mail->addAddress($_SESSION['email']);
$mail->isHTML(true);
  $mail->Subject = 'Your 2FA Verification Code';
  $mail->Body = "
    Hi {$_SESSION['username']},<br><br>
    Your 2FA verification code is: <strong>{$_SESSION['2fa_code']}</strong><br><br>
    This code will expire in 5 minutes.<br><br>
    Regards,<br>
    UPTM Disciplinary System
  ";

  // ☑ Send the email
  $mail->send();
```

Also, the 2FA code has time restriction to avoid its reuse and the session is kept under consideration to avoid reuse of the step maliciously. In fact, this attribute improves the security of the system, particularly, against the leakage of passwords and phishing.

3. SQL Prepared Statements (SQL Injection Prevention)

SQL injection is a hacking technique, in which users with malicious intentions attempt to exploit database queries with input fields. This system prevents such an attack by making use of pre-prepared statements of the SQL queries. Ready-to-use statements separate SQL logic and user inputs, therefore, making it impossible to insert malicious SQL code.

```
$checkQuery = "SELECT userID FROM users WHERE username = ? OR email = ?";
    $stmt = $conn->prepare($checkQuery);
    $stmt->bind_param("ss", $username, $email);
    $stmt->execute();
    $result = $stmt->get_result();
```

It is also applied in doing operations during a time of login, registration, a password reset, and case reporting. In each of these cases pre-written statements can make sure that user input is processed safely and the database is not threatened by injection attacks.

4. Session Hardening & Secure Logout (Session Hijacking Prevention)

The logged-in users and their roles are tracked with the help of sessions. This system keeps track of the sessions and ensures the existence and the validity of the sessions before allowing users to gain access to sensitive pages. It also sends an unauthorized user or an expired user to the log-in page.

```
session_start();

if (!isset($_SESSION['2fa_code']) || !isset($_SESSION['2fa_expiry'])) {
  echo "<script>
    alert('Session expired or unauthorized access.');
    window.location.href = '../index.html';
  </script>";
  exit;
}



if ($enteredCode == $_SESSION['2fa_code']) {
    // ☑ Redirect based on role
    switch ($_SESSION['role']) {
      case 'Admin':
        header('Location: ../admin/admin_dashboard.php');
        break;
```

It prevents hijacking sessions and allows one to use the same old sessions to breach the system, as it destroys sessions as soon as the user is checked by 2FA or resets a password. This takes precedence in sensitive systems like disciplinary record management system.

5. Role-Based Access Control (Enforcing Access Permission)

That is where the role-based redirection is implemented; the system will only allow the relevant pages to be available to every role, i.e.: Admin, Staff or Student, so that the sensitive data like disciplinary records or administration controls will not be available to an unapproved user.

```
switch ($_SESSION['role']) {
      case 'Admin':
        header('Location: ../admin/admin_dashboard.php');
        break;
      case 'Staff':
        header('Location: ../staff/staff_dashboard.php');
        break;
      case 'Student':
        header('Location: ../student/student_dashboard.php');
        break;
      default:
        header('Location: ../error.php');
    }
```

This system is used to ensure a high level of separation of privileges and protect critical functions. Such as, students can never edit cases and staff cannot administer the accounts of the admin. Role based access control implements the least privilege principle around the system.

6. Password Reset Verification (Identity Verification)

In case of an incident where a user forgets his password, the user will be required to authenticate himself via email. A random check-up code is created and ready to be sent through an email. This code must be filled in by the user before he or she changes his or her password. This does not allow a person to reset another user the password.

```
$verificationCode = rand(100000, 999999);

  // 🔍 Check in Users table (Admin/Staff)
  $stmt = $conn->prepare("SELECT userID, username FROM users WHERE email = ?");
  $stmt->bind_param("s", $email);
  $stmt->execute();
  $result = $stmt->get_result();

  $_SESSION['reset_userID'] = $user['userID'];
  $_SESSION['verification_code'] = $verificationCode;
```

The system handles two different types of accounts: Admin/Staff and Student and handles their password reset process. The codes are stored in session variables and expire after a short period of time to guarantee temporary access to the system and prevent the attack of brutality.

7.6 Conclusion

To conclude, the history of the creation of the Secure Student Disciplinary Record Management System stresses the importance of including powerful security into the management of sensitive academic and disciplinary data. In this chapter, it was mentioned that there are some important security features, which include password hashing, 2FA, session handling, access control, prepared statements, and secure password reset. All these functions play a very crucial role in ensuring user data security as well as the confidentiality, integrity and availability of the system.

Even in the instance of database breach, password hashing protects the user against unauthorized access; 2FA authenticates the identity in a manner that there could be no account breaches. Ready-made statements protect the system against one of the most frequent severe threats in web applications SQL injection attacks. Moreover, role-based access control and strict management of the sessions allow only authorized users to view particular pages or do some sensitive operations, which is in accordance with the principle of least privilege. The password reset process also enhances the security procedures since user identity is tested and only then a user is allowed to make any change.

All in all, the following security features prevent the system against potential cyber threats and contribute to the development of trust in it, as the users are guaranteed of the highest attention to their personal and disciplinary data in security concerns. Security, as emphasized in this chapter, is not merely a feature but it is a part of the system design, and more so where the applications touch sensitive academic and personal information. The integration of these security controls provides a user-centered, safe, and reliable environment to the system, which is aligned to current standards in cybersecurity.

8 TESTING

8.1 Introduction

Testing of the system was done so that all the features of the system are functioning correctly, users will be able to interact with the system in the same manner that it is expected to be, and security measures will be in place to make sure that sensitive data will not be accessed by unauthorized individuals. The strategy aims at testing the system in relation to accuracy, reliability and usability, and security levels of three user groups including Admin, Staff and Student.

Rather than using theoretical methods of tests, it was a practical approach that uses scenarios that are practical and user-friendly. This involves input data validation, user authentication testing, proper role-based access validation, report generation validation and verification of evidence uploads. Feedback on the end-users was solicited and particularly the staff and the administration members were consulted to ensure that the system addressed their requirements to operate.

8.2 Unit Testing

Unit testing focused on making sure that the different components of the system work as expected in isolation. Each module, for instance, login, registration, 2FA, reporting cases, viewing of cases, and password reset, was tested with valid and invalid inputs to make sure it is accurate, reliable, and secure. Unit testing allowed us to detect bugs at the earliest possible stage and ensured that each module would work correctly, not depending on other parts of the system. For instance, a login module was tested to ensure that correct credentials combined with 2FA give access, while wrong credentials or codes are properly blocked. The same is true for the registration modules of Staff and Students, which were tested for input validation, duplicate checking, and secure password hashing.

Module	Test Description	Input	Expected Output	Actual Output	Result
Login & 2FA	Validate login with correct/incorrect credentials	Username/password	Correct credentials trigger 2FA; wrong credentials rejected	As expected	Passed
2FA Verification	Validate entered code	Correct/incorrect code	Correct code allows dashboard access; wrong code rejected	As expected	Passed

Registration – Staff	Check inputs, duplicates, insert to DB	Username, email, password	Account created; duplicate errors triggered	As expected	Passed
Registration – Student	Check inputs, duplicates, insert to DB	Student ID, email, username	Account created; duplicates blocked	As expected	Passed
Case Reporting	Auto-fill student info by ID	Student ID input	Auto-fill Student Name, Faculty, Course	As expected	Passed
Case Reporting	Validate inputs, upload evidence	Case details & files	Data saved; file uploaded	As expected	Passed
View/Update Case	Update case details	Offense, description	Database updated securely	As expected	Passed
Password Reset	Verification code & new password	Registered email	Code sent; password updated	As expected	Passed
PDF Generation	Generate case report	Case ID	PDF contains all case info accurately	As expected	Passed

Table 9: Unit Testing Results

Observation:

Unit testing was successful because each module was proven to be functional and safe. There were no severe mistakes, and every module carried out the relevant tasks effectively.

8.3 Integration Testing

Integration testing was conducted to ensure that different modules are interacting with each other as desired and the data is flowing as planned. This was a needed measure since though various modules may be able to perform very well alone, when there are interrelations with other components of the system, bugs may emerge. Integration testing was done to test situations when a large number of modules are involved, e.g., login → 2FA → dashboard or password reset → verification → login. Role based access was also put to test in order to make sure that the users had access to only the relevant pages to their role. These tests ensured that the information integrity and security of the information held by the system are kept in the interactions between modules.

Scenario	Modules Involved	Test Steps	Expected Outcome	Result
Admin login → 2FA → Dashboard	Login, 2FA, Dashboard	Enter credentials → receive 2FA → enter code	Admin redirected to dashboard	Passed
Staff login → Report Case → View Case	Login, Report Case, View Cases	Staff login → report a case → view it	Case appears correctly in table	Passed
Student login → View Own Cases	Login, View Case	Student login → view cases	Only student's cases visible	Passed
Password reset → Login	Forgot Password, Reset Password, Login	Enter email → verify code → reset password → login	User logs in with new password	Passed
PDF Generation	View Case, PDF	Staff views case → generate PDF	PDF contains correct case info	Passed
Role-Based Access	All modules	Attempt unauthorized access	Unauthorized pages blocked	Passed

Table 10: Integration Testing Results

Observation:

The integration testing was used to verify the compatibility of the modules in the system. Users were able to do tasks that involved several modules without errors and security measures such as access control and data consistency were verified.

8.4 System Testing

The proposed testing of the Secure Student Disciplinary Record Management System was to include system testing of the entire system which included the overall functionality, overall performance, usability and security.

8.4.1 Functional Testing

This involves undertaking functional testing so that it can satisfy the functional requirements which include log in, case reporting, case updating, generation of PDFs, and password management. All the features were validated using both valid and non-valid inputs to make sure they act as anticipated in a real world.

Function	Test Description	Test Steps	Expected Outcome	Result
Role-Based Access	Admin, Staff, Student access	Login with each role	Only permitted pages accessible	Passed
Case Reporting	Add new case	Staff/Admin reports case	Case saved; auto-fill works	Passed
Case Update	Edit offense, status, description	Admin/Staff updates case	DB updated securely	Passed
Case Viewing	View assigned cases	Login → view case table	Correct cases displayed	Passed
PDF Report	Download PDF report	Select case → download PDF	PDF accurate	Passed
Evidence Upload	Upload images/PDF	Report case → upload file	Files uploaded & downloadable	Passed
Password Management	Reset password	Forgot password → verify → reset	Password updated; login successful	Passed
Registration	Staff & Student registration	Submit valid data	Account created; duplicates blocked	Passed
2FA Verification	Send code via email	Login	2FA code emailed; expires in 5 min	Passed

Table 11: System Functional Testing Results

8.4.2 Non-Functional Testing

Non-functional testing was used to make sure that the system passed the quality test that is assigned outside the substantive functionality like security, performance, usability, compatibility and availability.

Aspect	Test Description	Method	Expected Outcome	Result
Security	SQL injection protection	Input malicious SQL	Rejected; DB safe	Passed
Security	XSS prevention	Input scripts in forms	Script sanitized	Passed
Performance	Load handling	Multiple users simultaneously	System responsive	Passed
Usability	Ease of navigation	Users perform tasks	Interface intuitive	Passed
Compatibility	Browser test	Google Chrome, Microsoft Edge	Works correctly on all	Passed
Availability	Session management	Session timeout	Expired sessions log out	Passed

Table 12: System Non-Functional Testing Results

Observation:

System testing would see to it that the Secure Student Disciplinary Record Management System operates under normal, boundary and stress conditions as well as that the security mechanisms of 2FA, input validation and role-based access control are working properly.

8.5 Acceptance Testing

Acceptance testing was where real users would test the system in real-life situations as would be the case in real life. Feedback responses were desired and examined on Admin, Staff and Students to conclude that the system does bring out the expectations of those using it.

8.5.2 Alpha Testing

Tester	Role	Scenario	Feedback	Result
Admin	Admin	Update cases, generate PDF	Interface intuitive; dashboard clear	Passed
Staff	Staff	Report cases, view cases	Auto-fill and validations useful	Passed
Student	Student	View own case records	Accessible and clear	Passed

Table 13: Alpha Testing Results

Alpha testing indicated that internal users were able to easily carry out core operations and students were able to easily view records. This feedback was used to make minor adjustments to UI.

8.5.3 Beta Testing

User Group	Role	Scenario	Observation	Result
Staff	Staff	Daily case reporting	System reliable; no errors	Passed
Students	Student	Check case status	Information displayed correctly; secure	Passed
Admin	Admin	Monitor cases	Dashboard provides accurate statistics	Passed

Table 14: Beta Testing Results

Beta testing on the external users was a simulation of the real-world usage. It confirmed the stability of the system, accuracy and security of data and ensured it was ready to deploy.

8.5.4 Questionnaire Analysis (Post-Development)

After developing the Secure Student Disciplinary Record Management System, the usability test was carried out. The system requested responses about the system use among 50 responses consisting of students, staff people of Student Affairs Division, and admins. This survey will be aimed at discovering the usability, functionality, performance and satisfaction levels of the users on the system and areas that require improvements. To provide examples of the questions that the participants were asked, the screenshots of questions that were utilized in the survey created by Google Form will be displayed.

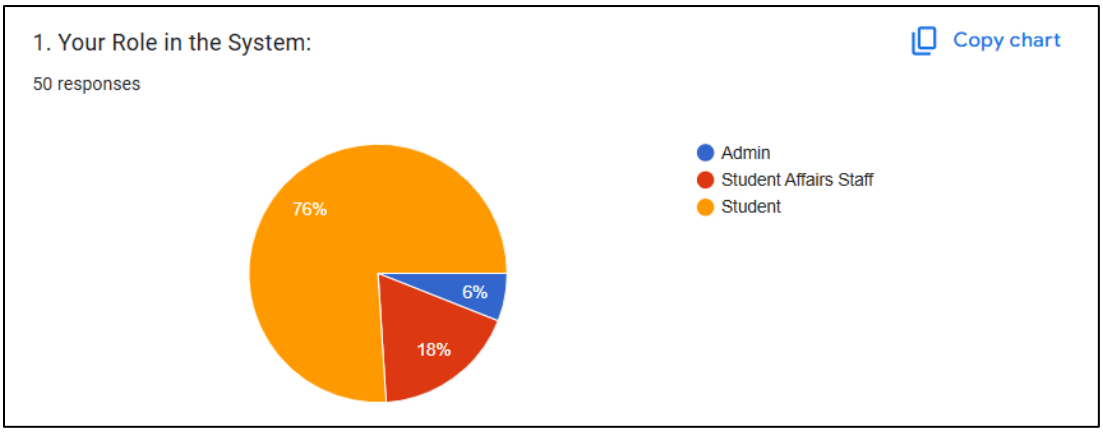


Figure 85: Questionnaire 1 – Participant Roles

Respondents breakdown was mainly students at 76%, then the staff of Student Affairs at 18%, and the rest at 6% which included the admins. This is a mirror of what the real-world situation entails given that students are the greatest users who will mainly view and manage their disciplinary records whereas the staff monitors and manages system functions. This gives a good understanding of the user experience as seen by a frequent user since students make a majority.

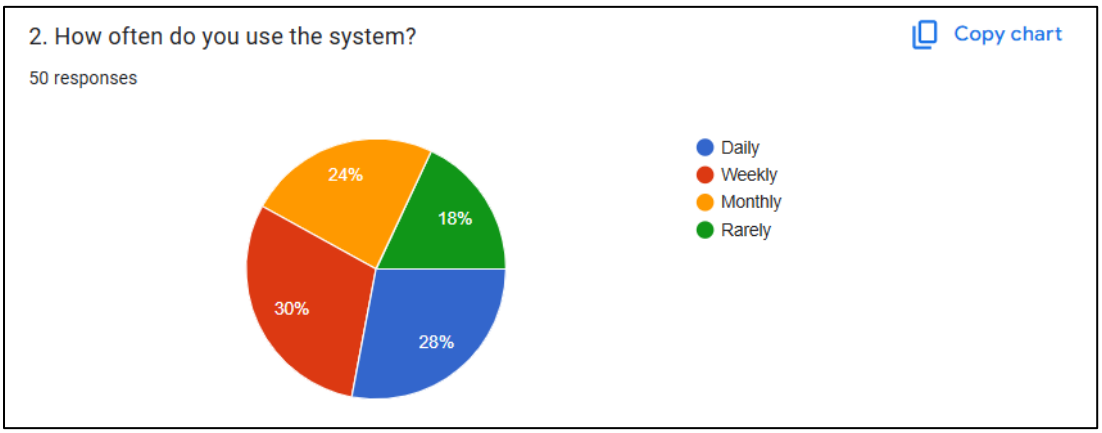


Figure 86: Questionnaire 2 – Frequency of System Usage

There were differences in patterns of usage where 28% used the system every day, 30% once a week, 24% once a month and 18% once in a long time. This fact indicates that the system is accommodative of occasional and frequent users. Based on the earlier suggestion that the usage rates were higher on weekends and days, it is evident that majority of users find this system convenient and applicable in the process of tracking or controlling disciplinary records.

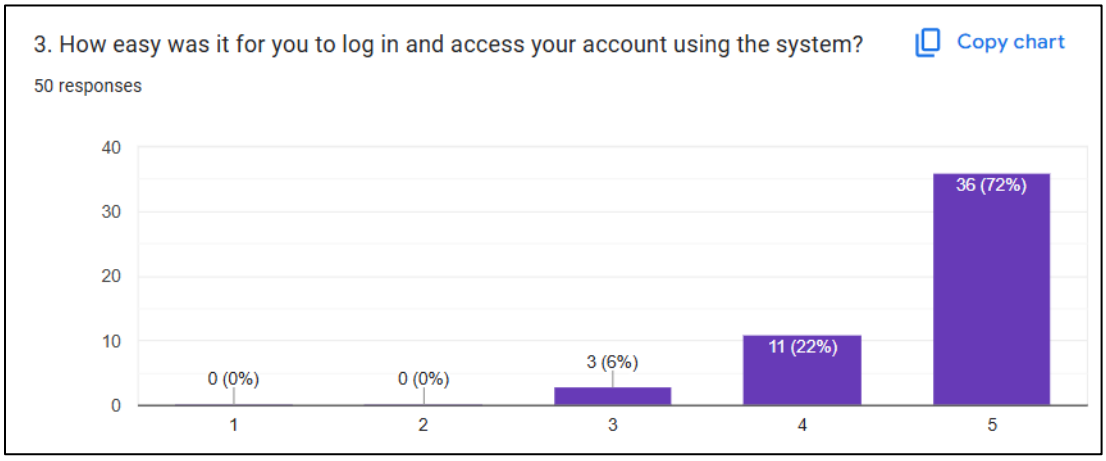


Figure 87: Questionnaire 3 – Ease of Login

The rating of login was very easy by 72% of all users, 4 by 22%, and 3 by 6%. This is a fair sign to show that the authentication system is easy to use and functional, but some users had slight problems. On the whole, the system is efficient in its access process and this helps create a good first impression about the system.

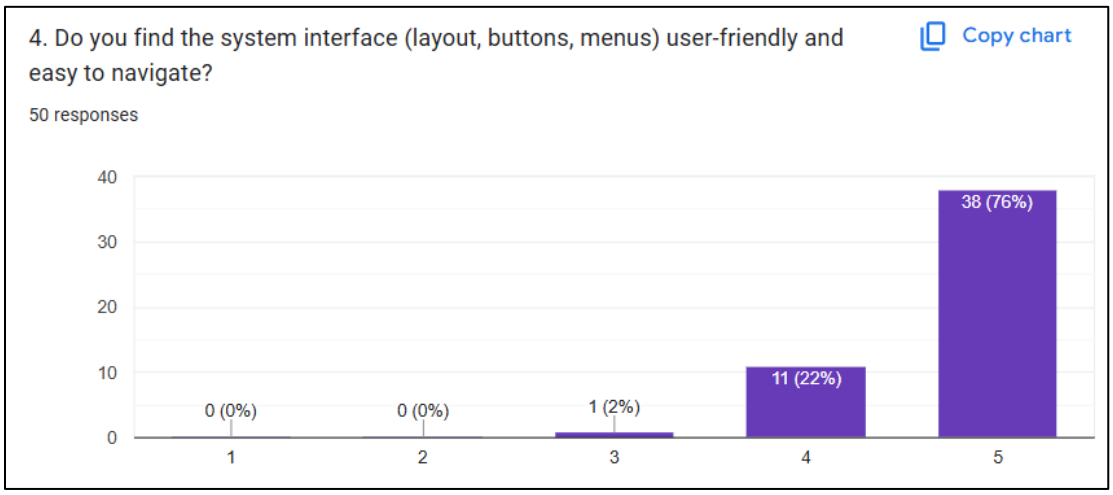


Figure 88: Questionnaire 4 – User Interface & Navigation

The interface is also highly accepted as 76% strongly agree that interface is user-friendly with 22% agreeing and 2% being neutral. The layout, menu, and buttons were self-explanatory and therefore, the system was easy to work with. The interface should be properly designed so that the user can carry out his or her job without the need to be confused or lose time.

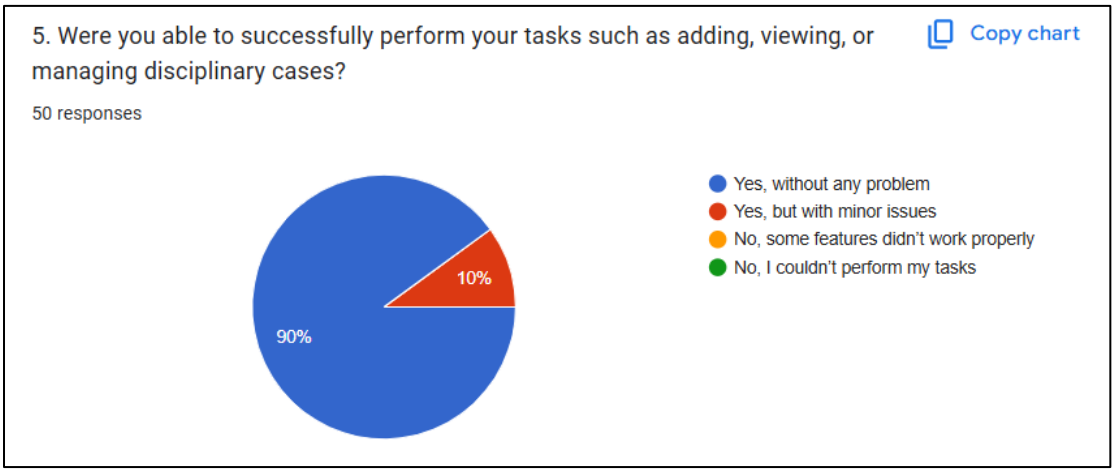


Figure 89: Questionnaire 5 – Task Completion

90% of the respondents said they could perform tasks such as adding, viewing, and managing disciplinary cases without problems, while minor problems were reported by 10% of the respondents. This means the system is functional for performing most of the core functionalities. Some minor problems can arise under certain usage scenarios, but as a rule, the Secure Student Disciplinary Record Management System supports the tasks well.

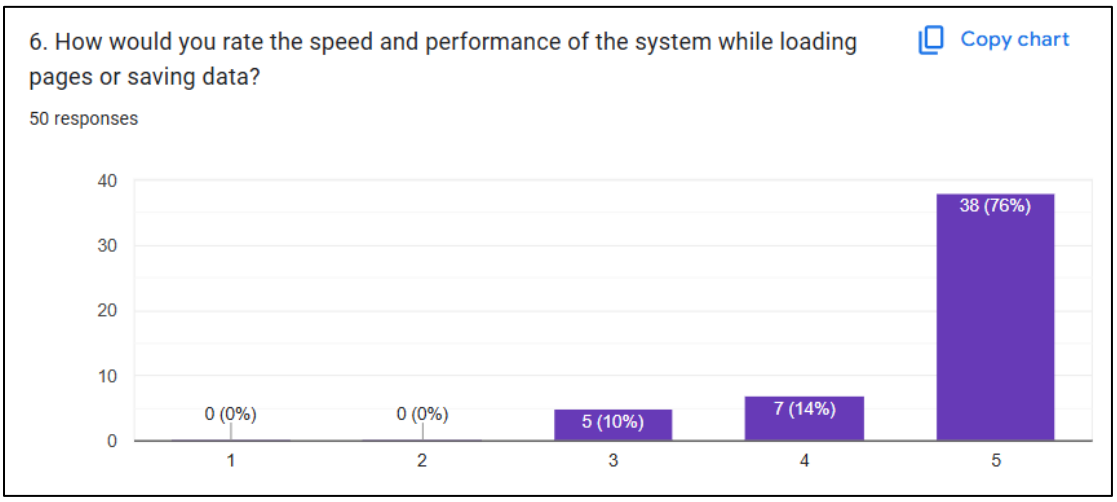


Figure 90: Questionnaire 6 – System Speed & Performance

Regarding performance, 76 percent of the respondents indicated the system to be very fast, 14 percent rated the system to be good, and 10 percent rated the system average. This is an indication that to the majority of the actual users, the system loads pages and stores data effectively. High performance is important aspect in ensuring user satisfaction, especially where administrative work is involved as latency can affect the working processes.

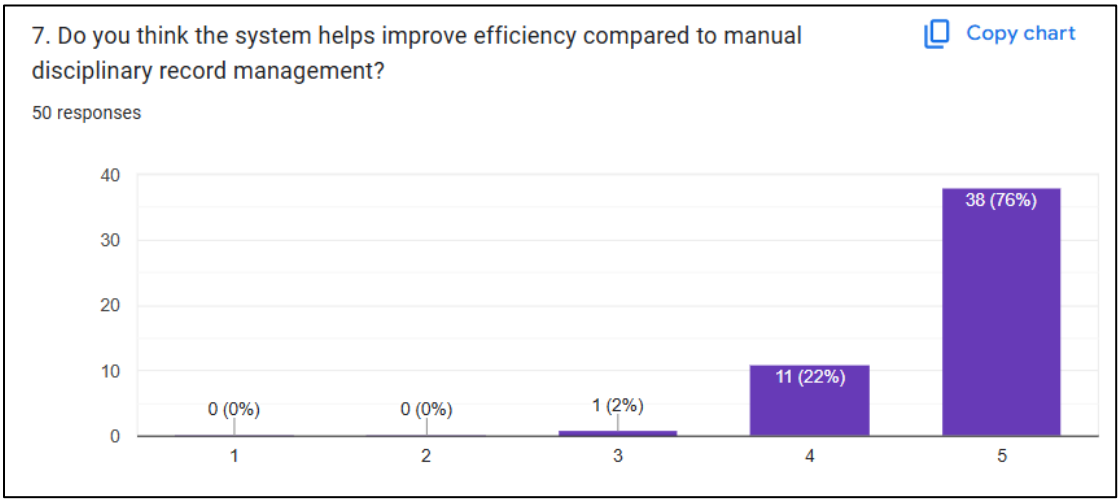


Figure 91: Questionnaire 7 – Efficiency vs Manual Process

The system is seen as having enhanced efficiency on a great scale: 76% strongly agreed, 22% agreed and 2% neutral. They value the system gets the records managed easily, unlike when the work was done manually because there are no mistakes, it is fast and makes the administration less difficult.

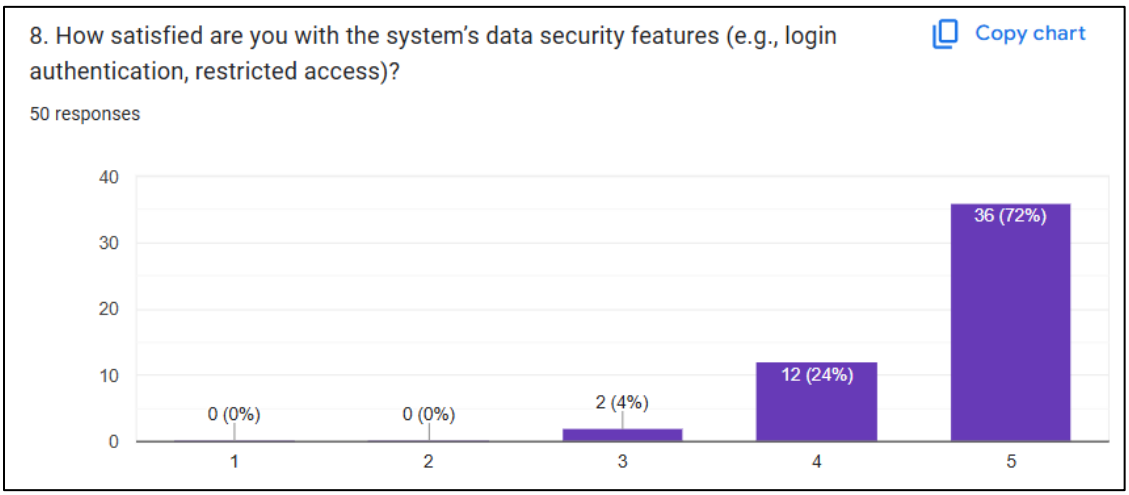


Figure 92: Questionnaire 8 – Satisfaction with Security

The users usually have confidence in the system security: 72 percent of users were extremely satisfied, 24 percent satisfied and 4 percent were neutral. Such functionalities as the authentications of users and the role-based access control can enable the users to be assured that such sensitive information on students is secure, the most vital requirement of a disciplinary record system.

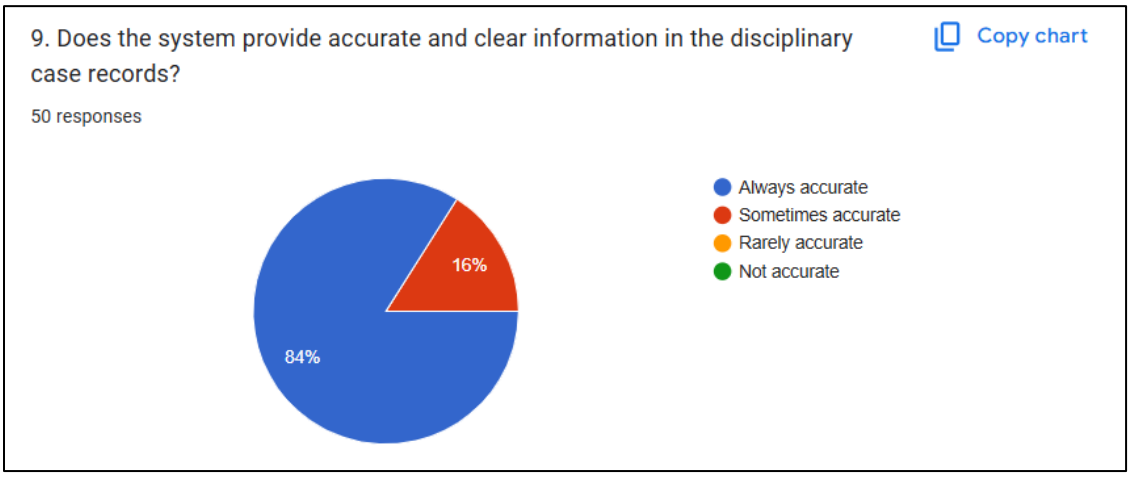


Figure 93: Questionnaire 9 – Accuracy of Records

The majority of the respondents answered that information contained in the disciplinary records is always accurate (84%), and 16 percent answered sometimes. This is an indicator of a high degree of data reliability. The correctness of the records is key to the transparency, sound decision-making, and trust between students and administration.

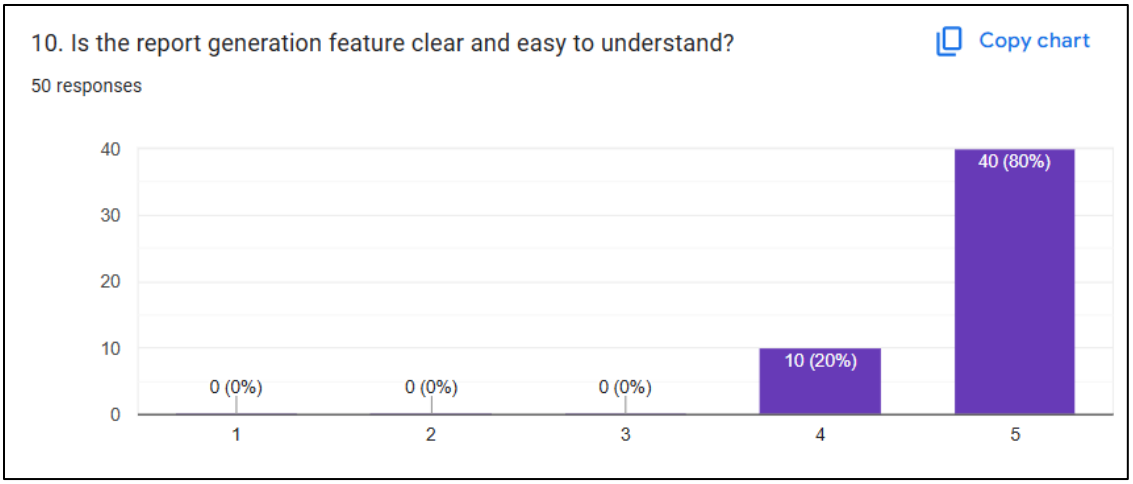


Figure 94: Questionnaire 10 – Report Generation

Creation of reports got the positive feedback as follows: 80 percent strongly agreed that it is clear and easy to understand with 20 percent agreeing. An easy reporting system enables employees and administrators to make right decisions in a more expedited manner thus increasing the efficiency of the administration.

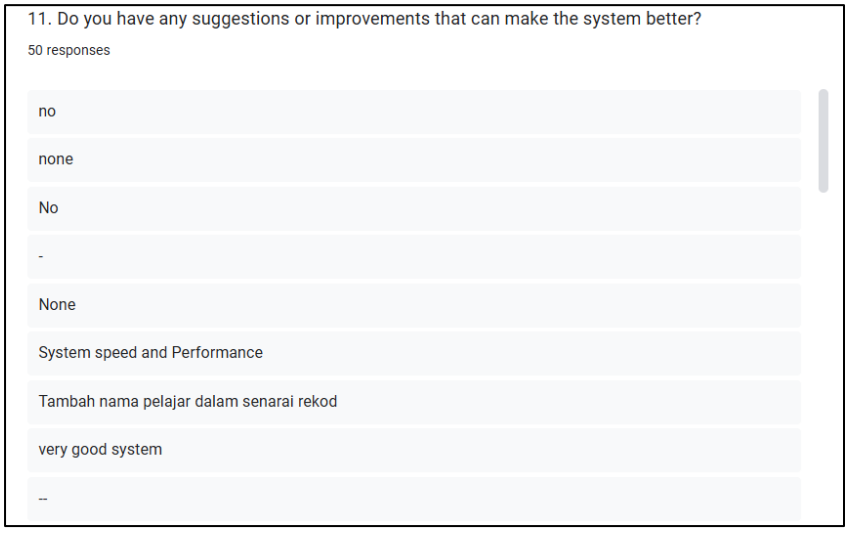


Figure 95: Questionnaire 11 – Suggestions & Improvements

The greatest number of users in this category reported that they did not have any recommendations; an indicator of satisfaction with the system. Others talked about minor concepts such as making the systems faster and including the name of students at the top of the case list to make it readable. In general, this group is an indication that the system is already functioning well with the majority of users.

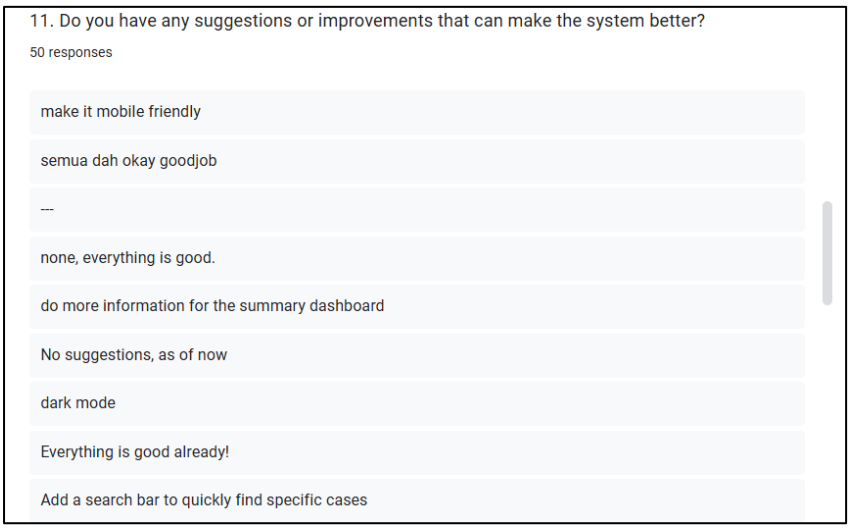


Figure 96: Questionnaire 11 – Suggestions & Improvements

This category involves appreciations and useful suggestions. Although numerous people claimed that everything was fine, some asked to be offered mobile-friendly access, a more elaborate dashboard, dark mode, and a search bar. The recommendations are convenience-based and primarily navigation-based.

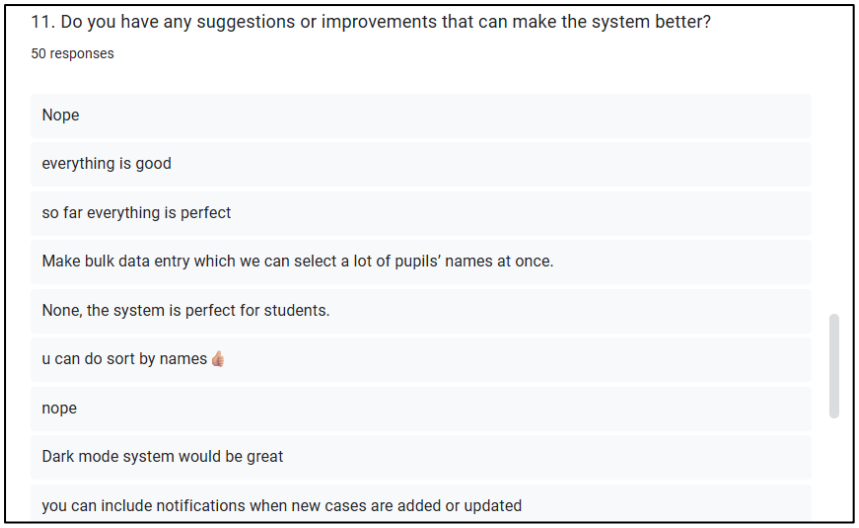


Figure 97: Questionnaire 11 – Suggestions & Improvements

These users were quite satisfied, but they also provided some helpful suggestions regarding the features that comprise bulk entry, name sorting, dark mode, and notifications. These would assist the staff to work efficiently and keep pace on any new or modified cases.

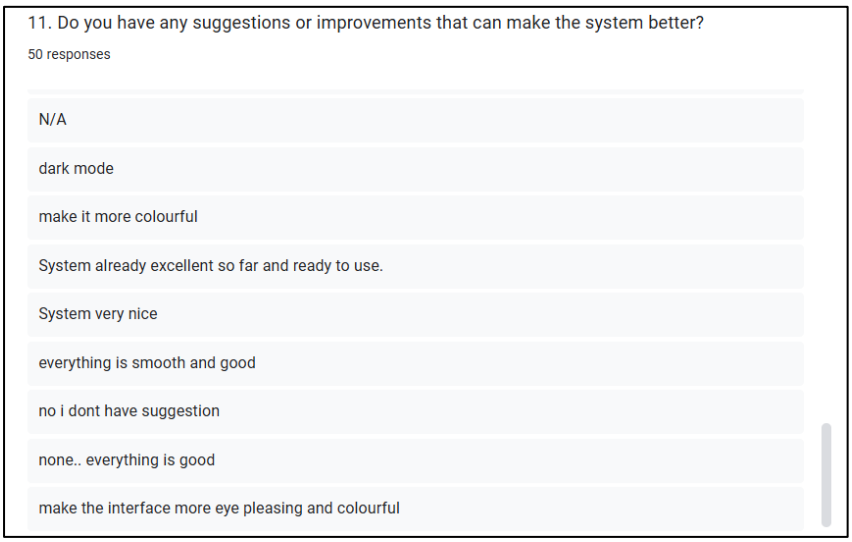


Figure 98: Questionnaire 11 – Suggestions & Improvements

The group mostly deals with the visual aspect of the system. The system was glorified by the user as being smooth, however, it was recommended to make the interface more visually appealing by being more colourful, including more features that are more appealing to the eye, and dark mode. These are not functional problems but only UI improvements.

Generally, all the four teams were happy about the work of the system and its capabilities. The recommendations primarily indicate the improvements that can be done in the future which may include improvement of UI, dark mode, mobile access, and search/sorting options which will further improve the user experience of anyone using the system.

The results of the questionnaire establish the fact that the Secure Student Disciplinary Record Management System effectively fulfils the needs of the users. The participants have rated it easy to use, and secure, efficient and reliable and have high support of tasks management, reporting and data accuracy. The user feedback shows a high rate of user satisfaction and makes viable suggestions on how it could be further improved, particularly, the interface customization, mobile access, and the introduction of more useful functions.

8.6 Conclusion

The security and reliability of the Secure Student Disciplinary Record Management System were only made reliable, secure, and efficient at an effective level when testing was a crucial step that made the system operational at the administration, staff of the Student Affairs Division, and the student level. The system was thoroughly tested at unit level up to acceptance testing level to identify bugs, prove key features and to check on overall user experience.

Various elements of the web application such as the login authentication system, 2FA system, role-based access, and him/herself modules were tested with the help of unit testing, and their functionality was checked. Integration testing also made sure that these pieces of it were relevant to each other particularly those that were intensive processes such as those dealing with a database interaction, updating of cases, and generating PDF reports. System testing also confirmed functional and non-functional components of the system such as performance, usability and security to ensure that it is specificationally valid.

Real user acceptance testing gave the most useful feedback. The alpha and beta testing indicated that the system is stable and can be put into practice. According to the post-development questionnaire that collected the reactions of 50 real users including the administrator, staff, and students, it can be concluded that the system is highly acceptable. Most of them rated the system as user friendly, safe, fast and useful in enhancing disciplinary records administration. Such recommendations as dark mode, search features, and UI improvement provide valuable directions towards the further development.

In general, testing confirms that the system is effective in addressing the issues of handling disciplinary records manually since it provides the digital platform with superior security, efficiency, and ease of use. It has also been shown that the system is already ready to be deployed, and only minor improvements have been proposed to be included in its future versions. This also proves the fact that the project has achieved its testing goals and it was suitable to address the needs of its potential users.

9 PROJECT MANAGEMENT

9.1 Introduction

This FYP2 involves project management as a massive aspect so that the formulation of the Secure Student Disciplinary Record Management System does not lack structure, organization, and effectiveness. This chapter provides a summary of the way the project was planned, scheduled, operated and controlled. These would be the WBS, Gantt chart and risk management plan. It will also comment on the success of the project according to the original plan and the changes which were made during the course of the project. The project management was good such that the system was delivered in due time and still fulfilled functionality and security requirements.

9.2 Project Schedule

The project plan was generated with the objective of subdividing all the tasks into manageable stages such that the system could be done in stages within the semester. The project schedule has been monitored on a regular basis and, in actual fact, certain activities have been longer than expected, particularly in the process of integration testing and security hardening. Overall, the project was kept on schedule with some setbacks; they were mitigated by the re-allocation of time and improvement of task prioritization.

9.2.1 Work Breakdown Structure

The Work Breakdown Structure of the project is categorized into six stages namely planning, design, development, testing, deployment and review. Under the planning stage, the scope of the project, objectives, stakeholders and requirements were identified. The design stage was to involve writing the database schema, architecture, user application and interface wireframes. The backend was developed, the frontend pages, and important features such as authentication, 2FA, generation of automated reports, and case reporting were developed. Unit testing, integration testing, system testing and acceptance testing were made up of this testing to provide stability and security. Deployment involved server set up, database set up, and setting up of final environment. Finally, there was the review phase to evaluate feedback and improve and finally document.

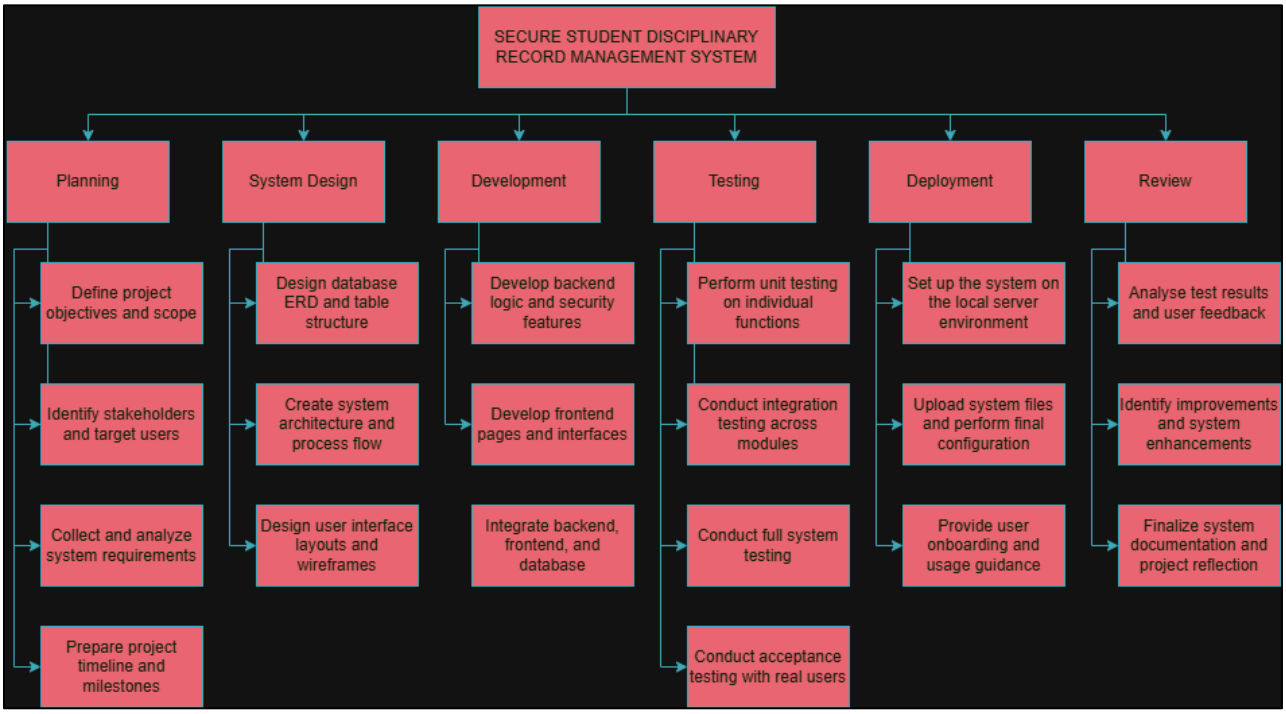


Figure 99: Work Breakdown Structure

9.2.2 Gantt Chart

Main Task	Subtask	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14
Planning	Define project objectives and scope														
	Identify stakeholders and target users														
	Conduct research and gather requirements														
	Prepare initial project schedule														
Design	Draft system architecture														
	Create ERD (Entity-Relationship Diagram)														
	Develop DFD (Data Flow Diagram)														
	Design user interface mockups														
Development	Implement authentication and user management modules														
	Develop admin, staff, and student functionalities														
	Integrate PDF report generation														
	Add security features (input validation, access control)														
Testing	Conduct unit testing for individual modules														
	Perform integration testing for combined modules														
	Execute system testing (functional and non-functional)														
	Address bugs and system issues														
Deployment	Set up server environment and database														
	Deploy system on live or test environment														
	Verify deployment and perform final checks														
	Provide initial user guidance														
Review	Conduct user acceptance testing (UAT)														
	Collect feedback from staff and students														
	Analyse questionnaire responses														
	Finalize documentation and prepare project report														

Table 15: Gantt Chart (Project Schedule)

Gantt chart gives one a clear picture of the project schedule, how every phase and activity is scheduled over the 14 weeks semester. It divides the project into six major stages, namely planning, design, development, testing, deployment, and review with each stage having its own subtasks and timelines. The chart presents what tasks are going to be performed simultaneously and what ones are going to be performed after others are completed beforehand; hence, it allows the team to organize their workflow much more efficiently. The Gantt chart shows the beginning and ending date of each task, therefore, it assists in making sure that significant milestones are achieved within the required time and marks the time period when additional focus might be necessary. Moreover, it will enable the team to monitor the progress, and any changes in case there is a delay and will act as a convenient way to allow the stakeholders to visualize the flow of a project through its start and finish.

Phase	**Subtasks/Activities**	**Week(s)**
Project Planning	Define project objectives, identify stakeholders and users, gather requirements, and prepare the project schedule.	Week 1 – Week 2
Design	Draft system architecture, create ERD, develop DFD, and design user interface mockups.	Week 3 – Week 4
Development	Implement authentication and user modules, develop admin, staff, and student functions, integrate PDF report generation, and add security features.	Week 5 – Week 10
Testing	Conduct unit testing, perform integration testing, execute system testing, and fix bugs and issues.	Week 10 – Week 12
Deployment	Set up server and database, deploy the system to the environment, verify deployment, and provide user guidance.	Week 12 – Week 13
Review	Conduct user acceptance testing, collect user feedback, analyze questionnaire responses, and finalize documentation.	Week 14

Table 16: Project Schedule Timetable

9.3 Risk Management

In developing the Secure Student Disciplinary Record Management System, there are some possible risks that can impact the project timeline, system functionality, and data security. All these risks were evaluated and mitigation strategies were to be developed to alleviate its effect. By foreseeing these risks, we were able to be proactive in solving the problems much earlier, continue the development process in a smooth manner, and have the system secure and reliable to all the users.

Risk	Analysis	Mitigation
Delay in gathering requirements from stakeholders	Could push back the planning and design phases, affecting overall timeline	Schedule meetings in advance, send reminders, and follow up with stakeholders regularly
Technical difficulties with implementing secure authentication and access controls	May cause development delays and potential security vulnerabilities	Allocate extra time for coding, testing, and debugging; use proven secure coding practices
System bugs or module errors during testing	Can affect functionality, user experience, and cause delays in deployment	Conduct thorough unit, integration, and system testing; document and fix bugs immediately
Poor user adoption or difficulty using the system	May result in complaints or underutilization of the system	Design user-friendly interface, provide clear guidance and training for staff and students
Data security risks (unauthorized access)	Could compromise sensitive student disciplinary records	Implement access control, input validation, and encryption for sensitive data
Server or deployment issues	Could prevent the system from running properly after launch	Prepare deployment checklist, test on live/test environment, and verify all configurations before launch

Table 17: Risk Management Plan

Based on the table above, it is clear that we have looked at all potential risks which were prudently put in mind and counteractions against them were already in place to ensure that their impact was minimized. The majority of these risks were addressed without having much influence on the project and no significant problem was faced in the process of development. Such was the proactive strategy that made sure that the system was ready and operational and in time to the staff and students of the Student Affairs Division.

9.4 Conclusion

The project of the Secure Student Disciplinary Record Management System was prepared and introduced according to the planned activity and schedule as it was projected in the Work Breakdown Structure and the Gantt chart. The project was implemented in a sequential fashion involving the planning and design, development, testing, deployment, as well as the review processes. The project schedule has assisted the group members in being organized in terms of effective utilization of resources and completion of the tasks before the due date. As a rule, the project has been managed strictly basing on the initial plan as some small changes were necessary to face the unforeseen challenges.

Risk management was one of the most contributory factors of the success of the project. The risks associated were diagnosed, assessed and mitigation measures against them outlined to ensure that the consequences in case this occurred were minimised. As a result, through the proactive approach, there were no significant problems that arose, and things proceeded in a smooth manner. This indicates that proper project management, effective planning, and risk mitigation should be done to present a working and secure system within the stipulated time.

10 CONCLUSION

10.1 Introduction

The design of the Secure Student Disciplinary Record Management System was to establish a centralized, safe, and effective system of handling the disciplinary related cases of students at Universiti Poly-Tech Malaysia (UPTM). This chapter also contemplates the achievement of the objectives of the project, constraints, the lesson learned, and possible areas of improvement that can be made. It also identifies the input of the system in enhancing the management of records and decision-making process in the university.

10.2 Achievement

By offering a secure and functional online platform, the system could meet its most important objectives since it serves staff and students that have to deal with disciplinary matters. The reviewed objectives are listed below and their achievement is evidenced.

10.2.1 To develop a centralized and secure web-based disciplinary record system that enables efficient creation, updating, and management of student misconduct cases.

The initial goal of the development was to have a centralized and secure web-based system of disciplinary records that would facilitate easy creation, updating and maintenance of cases of misconduct in students. This was achieved to the latter since in the system, the staff and the admin can create, edit and manage disciplinary records in a single centralized platform. It has been evidenced by functional modules of adding new cases, updating the old cases and searches with the disciplinary history of the students.

10.2.2 To implement a secure login and role-based access control system that ensures only authorized users can access and manage sensitive disciplinary data.

The second goal was to implement a secure login and role-based access control system, so that access to the disciplinary data and management of this data is restricted to only those users who are authorized. This was accomplished through integrating secure authentication, password hashing, and role-based permissions for Admin, Student Affairs staff, and students. It prevents unauthorized access, thus guaranteeing the confidentiality and integrity of data.

10.2.3 To provide tools for structured tracking and automated reporting to improve transparency and efficiency.

The third goal was to offer structured tracking tools that have automated reporting to promote transparency and efficiency. This objective can be met using the system by generating reports automatically based on the stored data as soon as the user clicks on the button "Download Report." The user starts the download but all the data is compiled and formatted by the system therefore, it achieves the automated reporting feature.

10.3 Constraint and Limitation

Although the objectives have been met, some obstacles were experienced. The system is not mobile responsive; it can also limit some of the access using smartphone or tablet. The entry of bulk data is still manual, and this could be slow when it comes to processing a great number of students. Other additions such as notifications, better dashboard analytics and customization of the interface were proposed by users though they could not be made because of time and resource limitations.

10.4 Future Work and Recommendation

Although the Secure Student Disciplinary Record Management System has managed to fulfil its objectives by offering a functional, workable and safe platform on disciplinary records management, there is always more that can be done to improve efficiency, usability, and other effects on the Student Affairs Division and the students. Future research can thus be focused on the work to improve the efficiency, usability, and overall effects of the System on the Student Affairs Division and students. The system would further decrease manual work by adding the features that will automize the synchronization with the university portal, show the present real-time notifications, and improve analytics dashboards. Such improvements would not only streamline the disciplinary record management process but also enlighten the improved decision-making and transparency which would render the system meaningful and useful in the long run.

10.4.1 Integration with University Student Portal

The first improvement that can be achieved is to link the system with the overall student portal of the university. Here, automatic synchronization of student information in the university database is possible and removes the manual process of registering students to minimize errors. Administrative activities would be quicker, more precise and the system would be linked to the records.

10.4.2 Real-Time Notifications

The other feature that is recommended is real-time notifications: to automatically inform the user concerned in case of a case creation, update or resolution. Notifications will be instantaneous and this will ensure that staff can respond promptly to incidents and their record keeping is up to date assisting with communication and accountability in the university.

10.4.3 Enhanced Analytics Dashboard

The system can also be enhanced with a better analytics dashboard, which will provide disciplinary patterns in the form of graphics. As an illustration, data in the form of number of cases per month or category may be displayed, which is easy to visualize the staff tendencies and areas to be used as a point of concern. These visual clues would serve the purpose of data-driven actions, which would enable the Student Affairs Division to implement preventative actions and will allow them to evaluate the efficiency of their disciplinary policies.

10.5 Conclusion

The implementation of the Secure Student Disciplinary Record Management System has had the capacity to support its key targets: to have a single and secure location to manage the student disciplinary records in an effective and efficient manner. The system allows authorized users to make, revise, and track cases and sensitive data can be stored safely using the implementation of role-based access and secure log-in solutions. The system has introduced case tracking and reporting systems that would assist staff to track the trends and generate reports that will be used to make improved decisions and internal review processes. All in all, the system can enhance efficiency, transparency, and accountability in the entire Student Affairs Division and prove it to be beneficial both to the staff and students themselves.

The security of the data, the presence of an intuitive interface, and automated reporting were some of the challenges in the entire project. This was resolved through proper planning, trial and error, and risk management policies which further increased the reliability and functionality of the system. Among the learnings is the need to have clear requirements, to test early and also to take into account user feedback during the design process. The next incorporation of the system in the university portal, the use of real-time notifications as well as the additional expansion of the analytics dashboard will significantly contribute to the system of increased utility and usefulness. This project helped in resolving real world, practical administrative issues and also contributed to body of knowledge on how to develop secure web-based management systems in a university setting.

Appendix A – Requirements Specification Document

I. Project Source Code (GitHub Link)

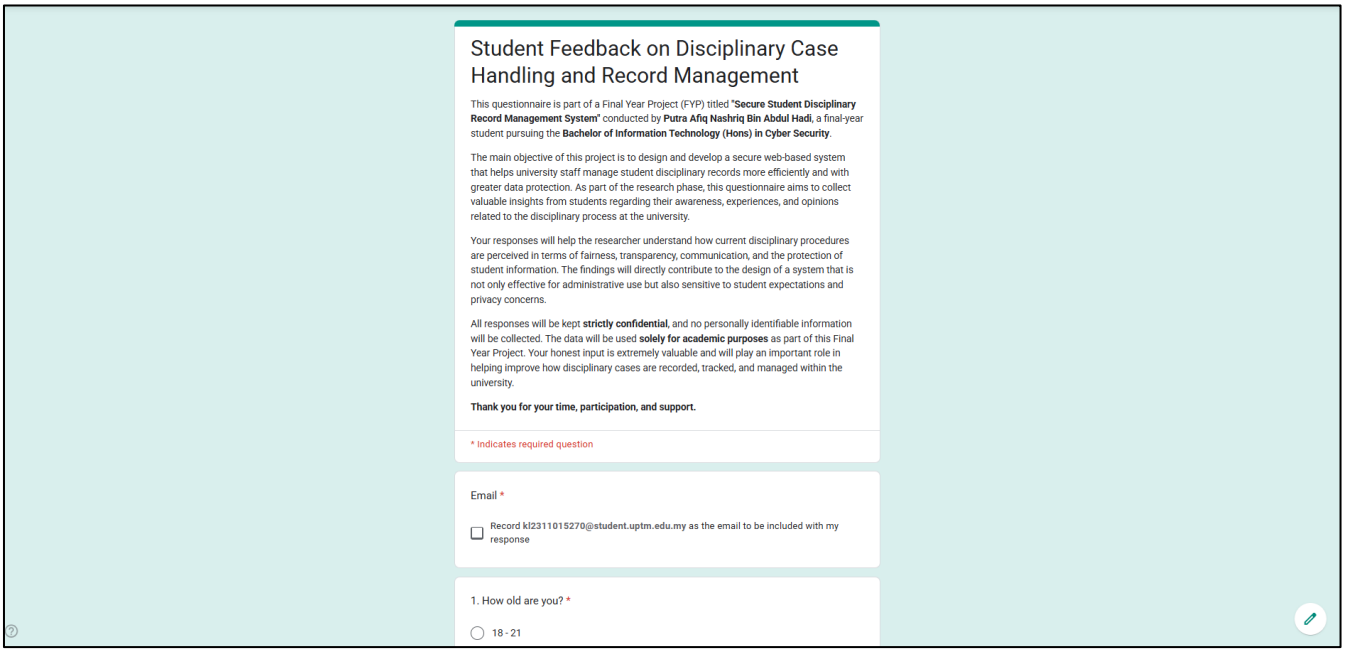
Secure Student Disciplinary Record Management System
https://github.com/afiqnashriq/student-disciplinary-record-ms

II. Demonstration Video (YouTube Link)

Secure Student Disciplinary Record Management System Demonstration Video
https://youtu.be/PPNu0Zx4GAU

Appendix B – Questionnaires

I. Questionnaire Pre-Development



Student Feedback on Disciplinary Case Handling and Record Management

This questionnaire is part of a Final Year Project (FYP) titled **"Secure Student Disciplinary Record Management System"** conducted by **Putra Afiq Nashriq Bin Abdul Hadi**, a final-year student pursuing the **Bachelor of Information Technology (Hons) in Cyber Security**.

The main objective of this project is to design and develop a secure web-based system that helps university staff manage student disciplinary records more efficiently and with greater data protection. As part of the research phase, this questionnaire aims to collect valuable insights from students regarding their awareness, experiences, and opinions related to the disciplinary process at the university.

Your responses will help the researcher understand how current disciplinary procedures are perceived in terms of fairness, transparency, communication, and the protection of student information. The findings will directly contribute to the design of a system that is not only effective for administrative use but also sensitive to student expectations and privacy concerns.

All responses will be kept **strictly confidential**, and no personally identifiable information will be collected. The data will be used **solely for academic purposes** as part of this Final Year Project. Your honest input is extremely valuable and will play an important role in helping improve how disciplinary cases are recorded, tracked, and managed within the university.

Thank you for your time, participation, and support.

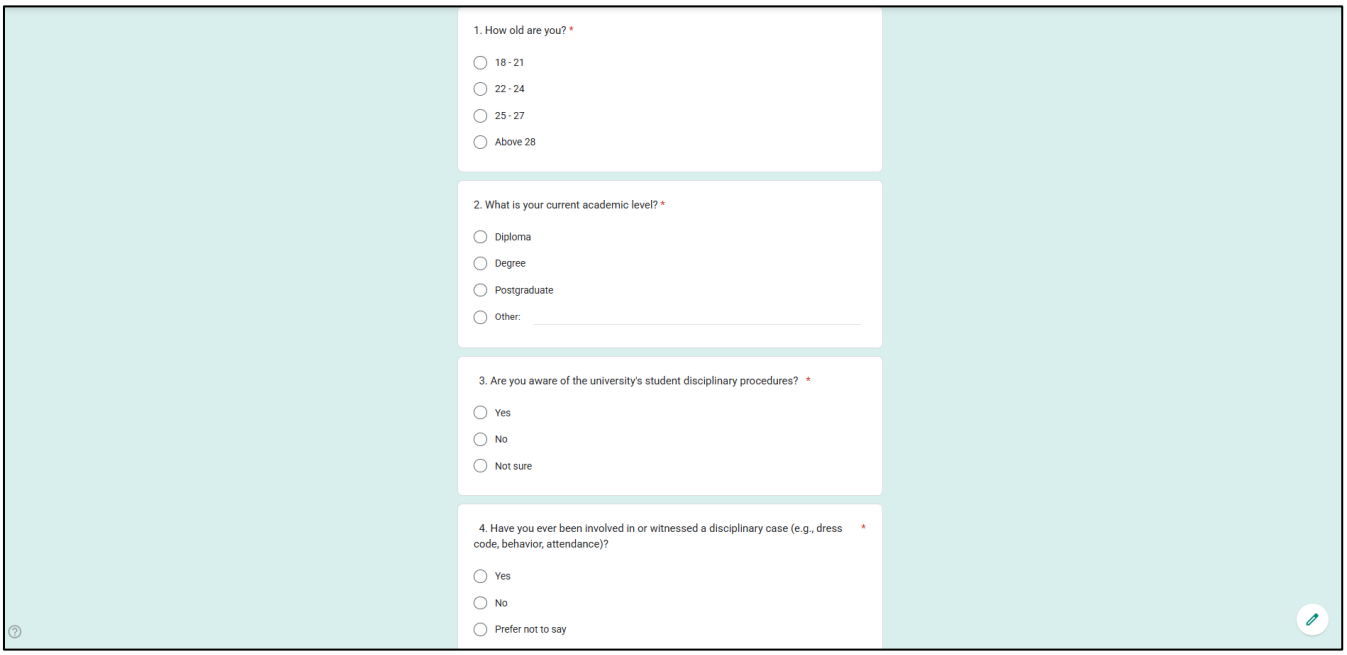
* Indicates required question

Email *

Record kl2311015270@student.uptm.edu.my as the email to be included with my response

1. How old are you? *

18 - 21



1. How old are you? *

18 - 21

22 - 24

25 - 27

Above 28

2. What is your current academic level? *

Diploma

Degree

Postgraduate

Other:

3. Are you aware of the university's student disciplinary procedures? *

Yes

No

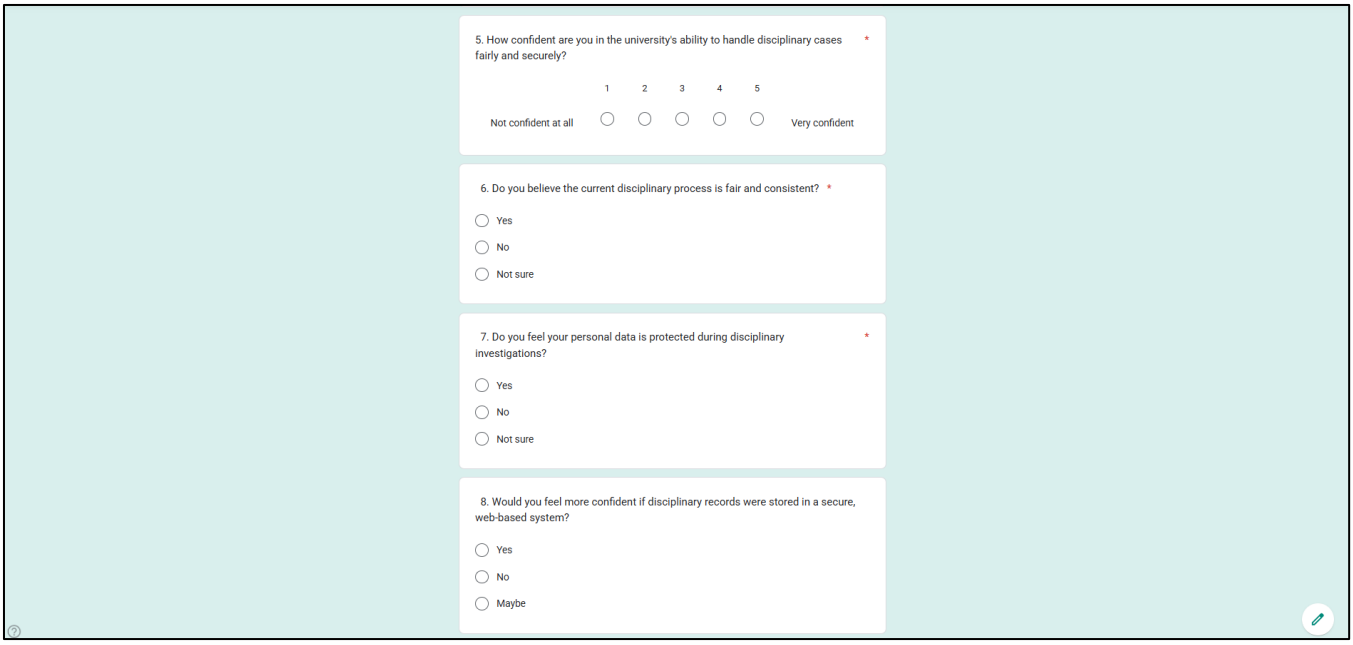
Not sure

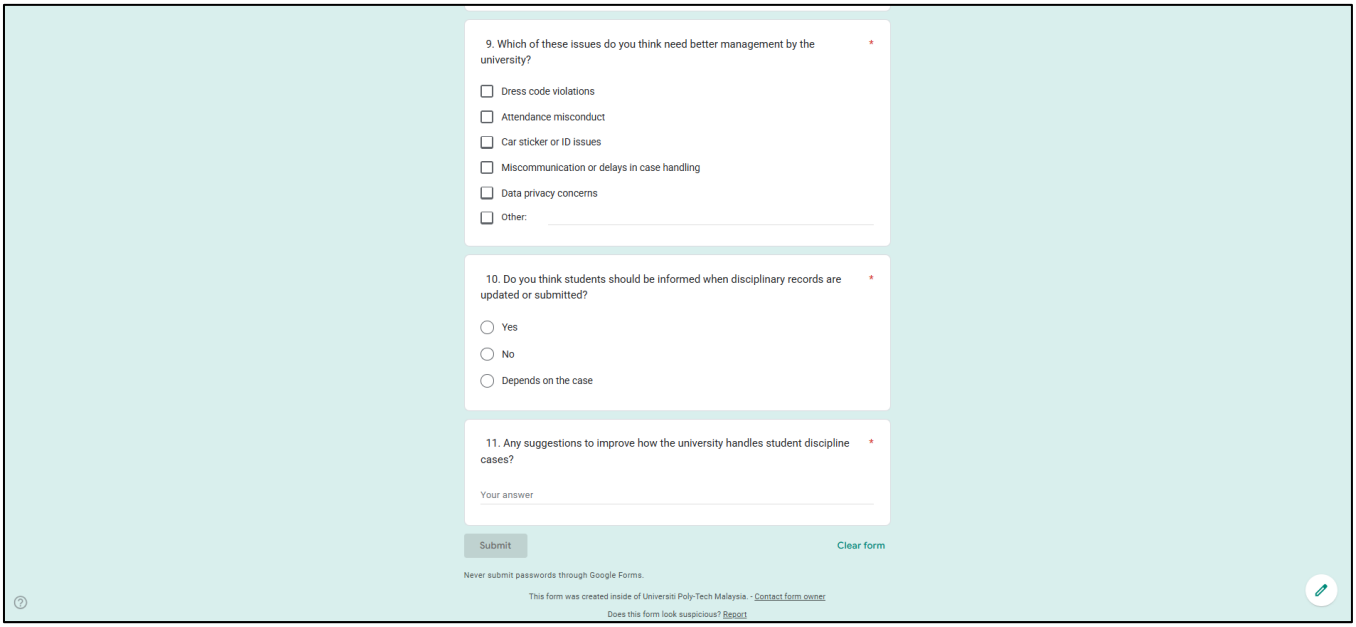
4. Have you ever been involved in or witnessed a disciplinary case (e.g., dress code, behavior, attendance)? *

Yes

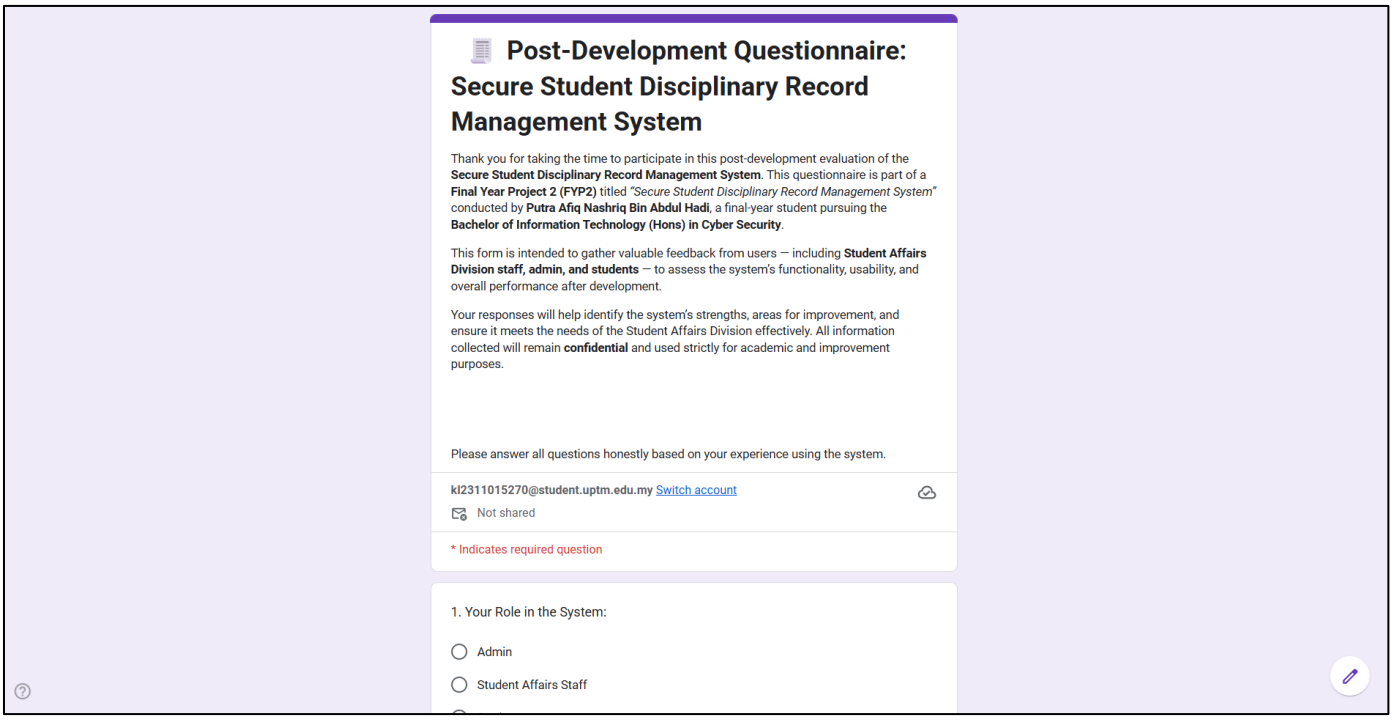
No

Prefer not to say


5. How confident are you in the university's ability to handle disciplinary cases fairly and securely? *
1 2 3 4 5
Not confident at all
Very confident
6. Do you believe the current disciplinary process is fair and consistent? *
Yes
No
Not sure
7. Do you feel your personal data is protected during disciplinary investigations? *
Yes
No
Not sure
8. Would you feel more confident if disciplinary records were stored in a secure, web-based system?
Yes
No
Maybe


9. Which of these issues do you think need better management by the university? *
Dress code violations
Attendance misconduct
Car sticker or ID issues
Miscommunication or delays in case handling
Data privacy concerns
Other:
10. Do you think students should be informed when disciplinary records are updated or submitted? *
Yes
No
Depends on the case
11. Any suggestions to improve how the university handles student discipline cases? *
Your answer
Submit
Clear form
Never submit passwords through Google Forms.
This form was created inside of Universiti Poly-Tech Malaysia. - Contact form owner
Does this form look suspicious? Report

II. Questionnaire Post-Development



Post-Development Questionnaire: Secure Student Disciplinary Record Management System

Thank you for taking the time to participate in this post-development evaluation of the **Secure Student Disciplinary Record Management System**. This questionnaire is part of a **Final Year Project 2 (FYP2)** titled *"Secure Student Disciplinary Record Management System"* conducted by **Putra Afiq Nashriq Bin Abdul Hadi**, a final-year student pursuing the **Bachelor of Information Technology (Hons) in Cyber Security**.

This form is intended to gather valuable feedback from users — including **Student Affairs Division staff, admin, and students** — to assess the system's functionality, usability, and overall performance after development.

Your responses will help identify the system's strengths, areas for improvement, and ensure it meets the needs of the Student Affairs Division effectively. All information collected will remain **confidential** and used strictly for academic and improvement purposes.

Please answer all questions honestly based on your experience using the system.

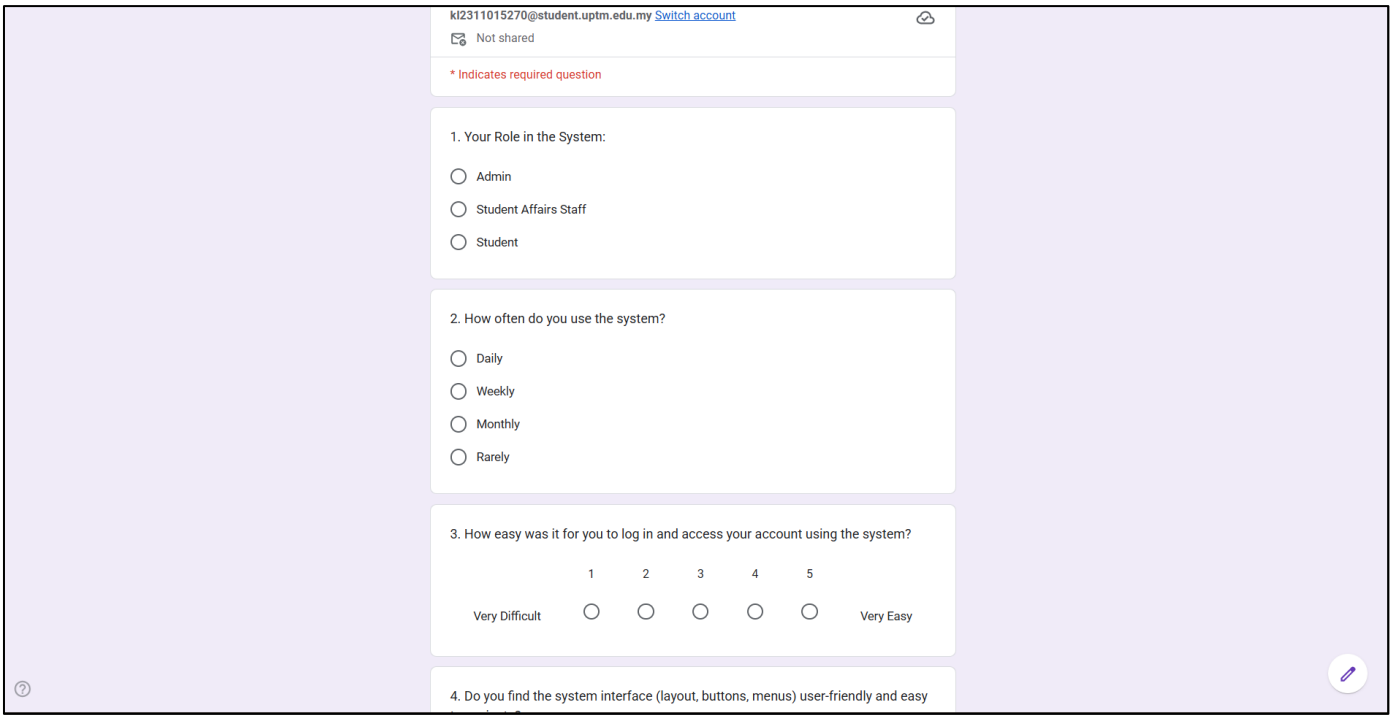
kl2311015270@student.uptm.edu.my Switch account

Not shared

* Indicates required question

1. Your Role in the System:

- Admin
- Student Affairs Staff



kl2311015270@student.uptm.edu.my Switch account

Not shared

* Indicates required question

1. Your Role in the System:

- Admin
- Student Affairs Staff
- Student

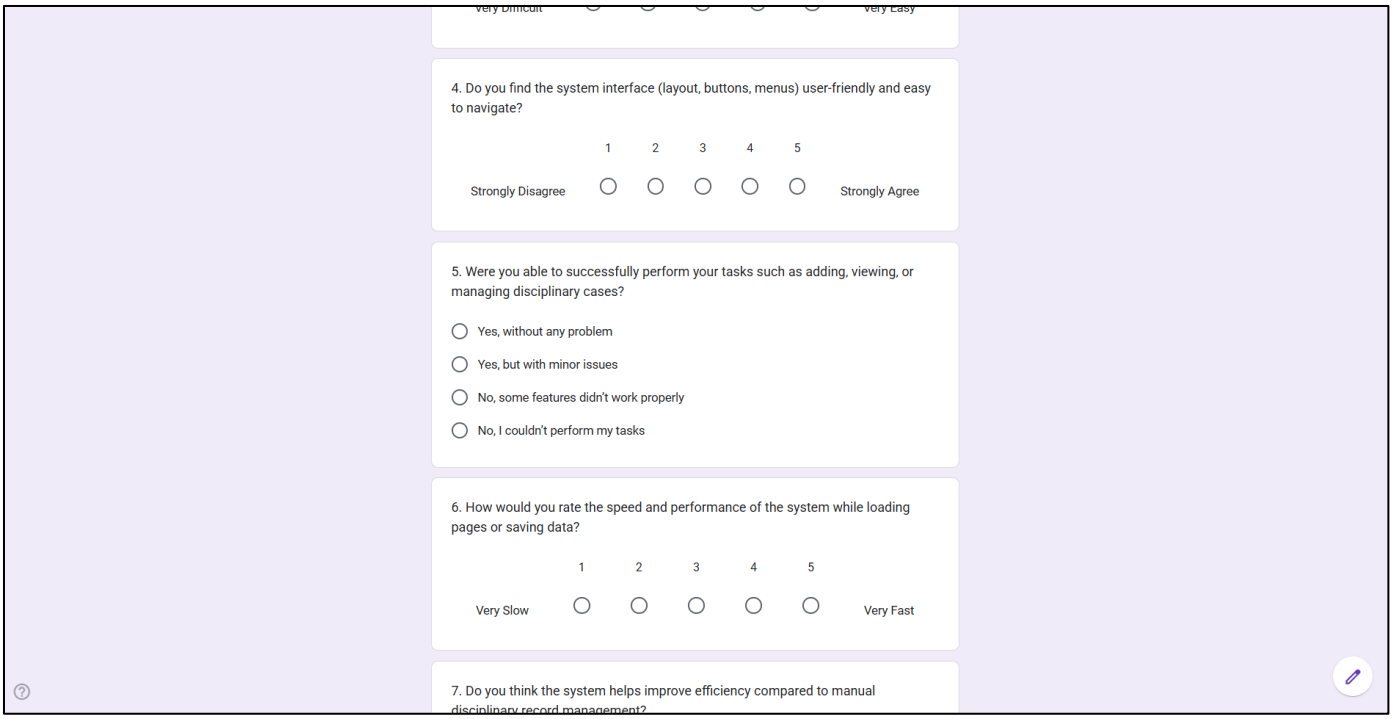
2. How often do you use the system?

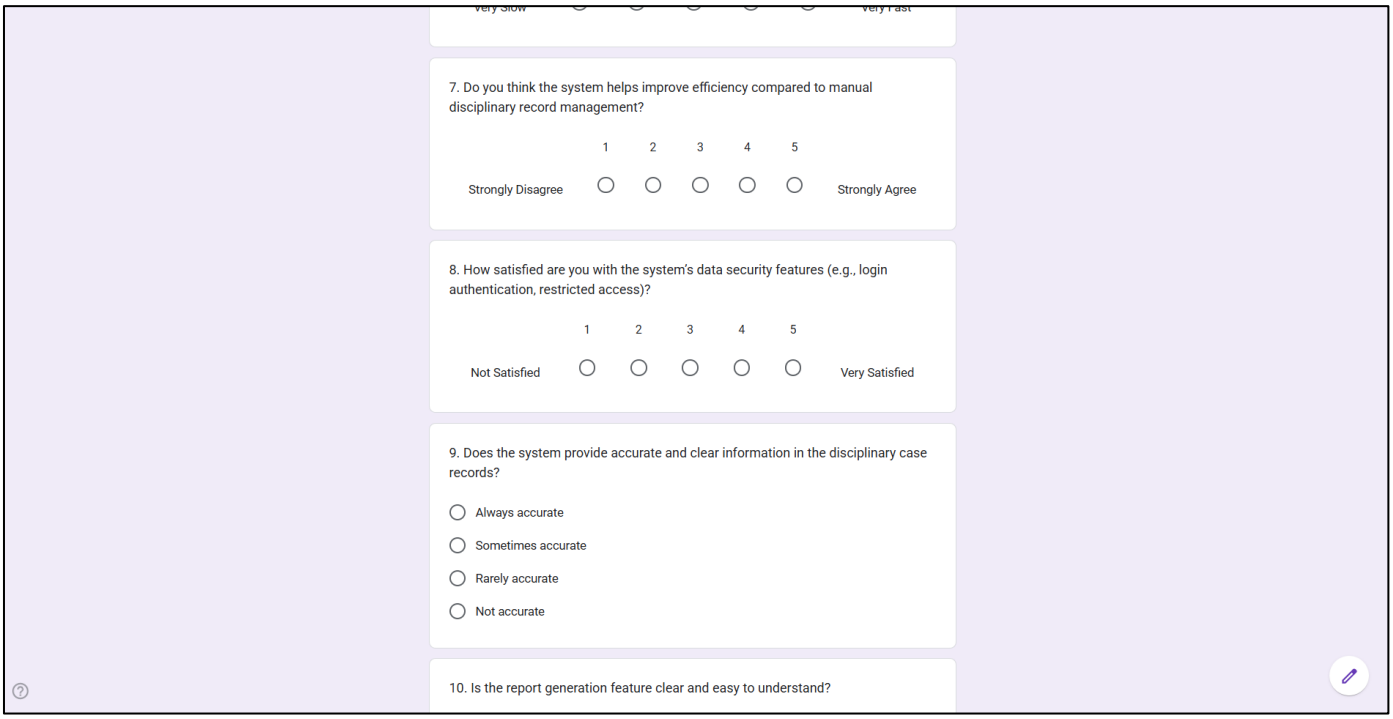
- Daily
- Weekly
- Monthly
- Rarely

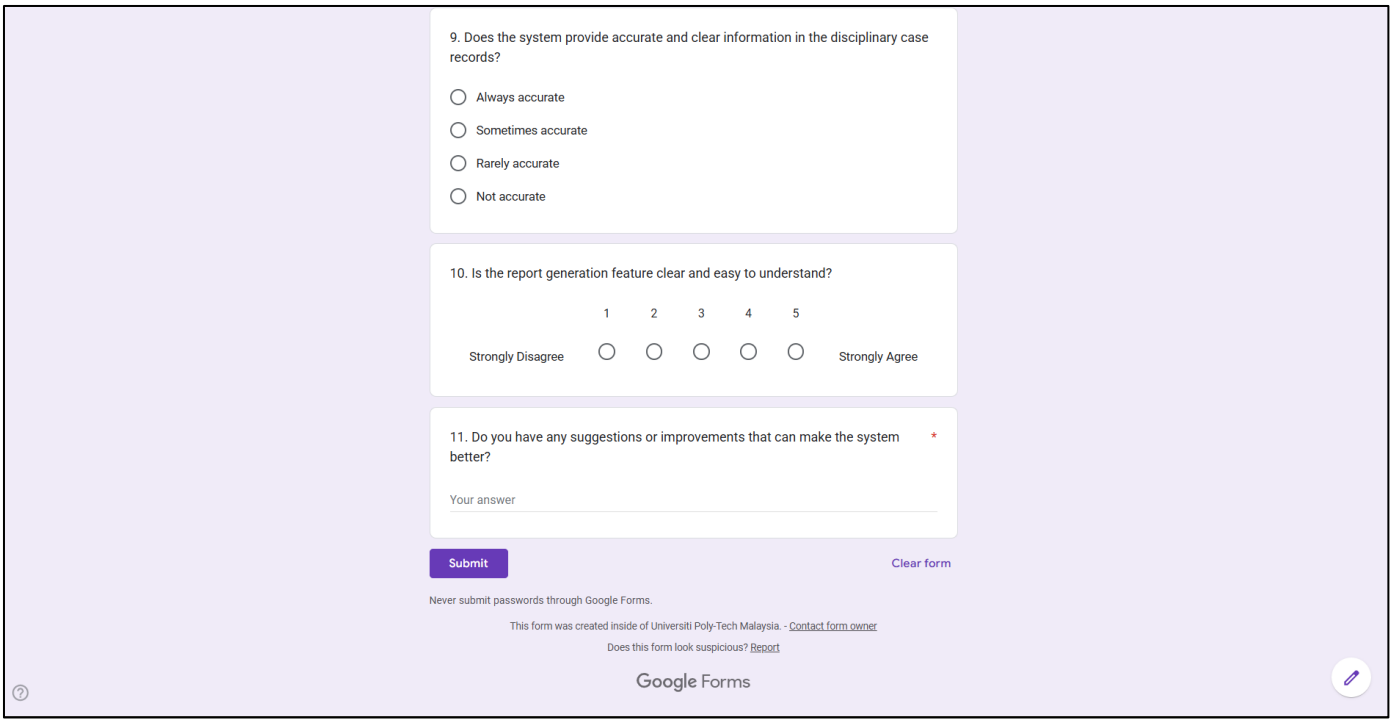
3. How easy was it for you to log in and access your account using the system?

	1	2	3	4	5	
Very Difficult	○	○	○	○	○	Very Easy

4. Do you find the system interface (layout, buttons, menus) user-friendly and easy

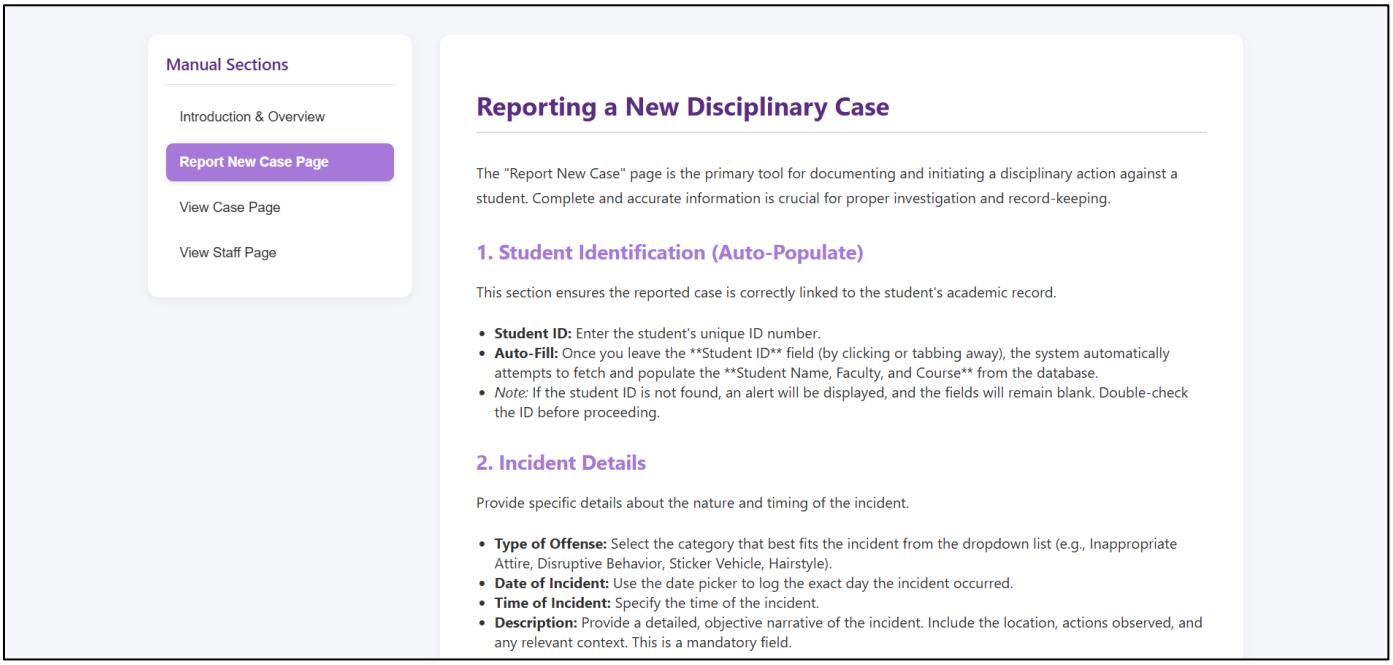

Very Difficult
Very Easy
4. Do you find the system interface (layout, buttons, menus) user-friendly and easy to navigate?
1 2 3 4 5
Strongly Disagree
Strongly Agree
5. Were you able to successfully perform your tasks such as adding, viewing, or managing disciplinary cases?
Yes, without any problem
Yes, but with minor issues
No, some features didn't work properly
No, I couldn't perform my tasks
6. How would you rate the speed and performance of the system while loading pages or saving data?
1 2 3 4 5
Very Slow
Very Fast
7. Do you think the system helps improve efficiency compared to manual disciplinary record management?

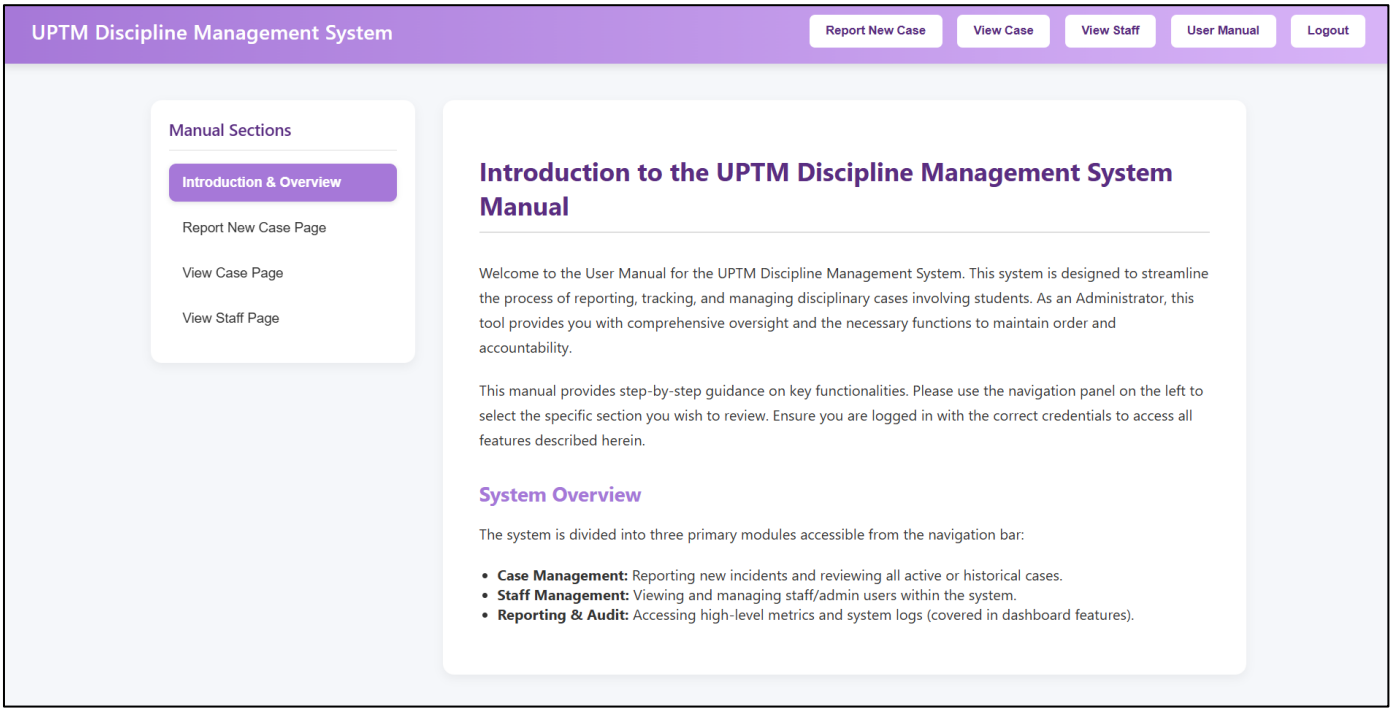

Very Slow
Very Fast
7. Do you think the system helps improve efficiency compared to manual disciplinary record management?
1 2 3 4 5
Strongly Disagree
Strongly Agree
8. How satisfied are you with the system's data security features (e.g., login authentication, restricted access)?
1 2 3 4 5
Not Satisfied
Very Satisfied
9. Does the system provide accurate and clear information in the disciplinary case records?
Always accurate
Sometimes accurate
Rarely accurate
Not accurate
10. Is the report generation feature clear and easy to understand?

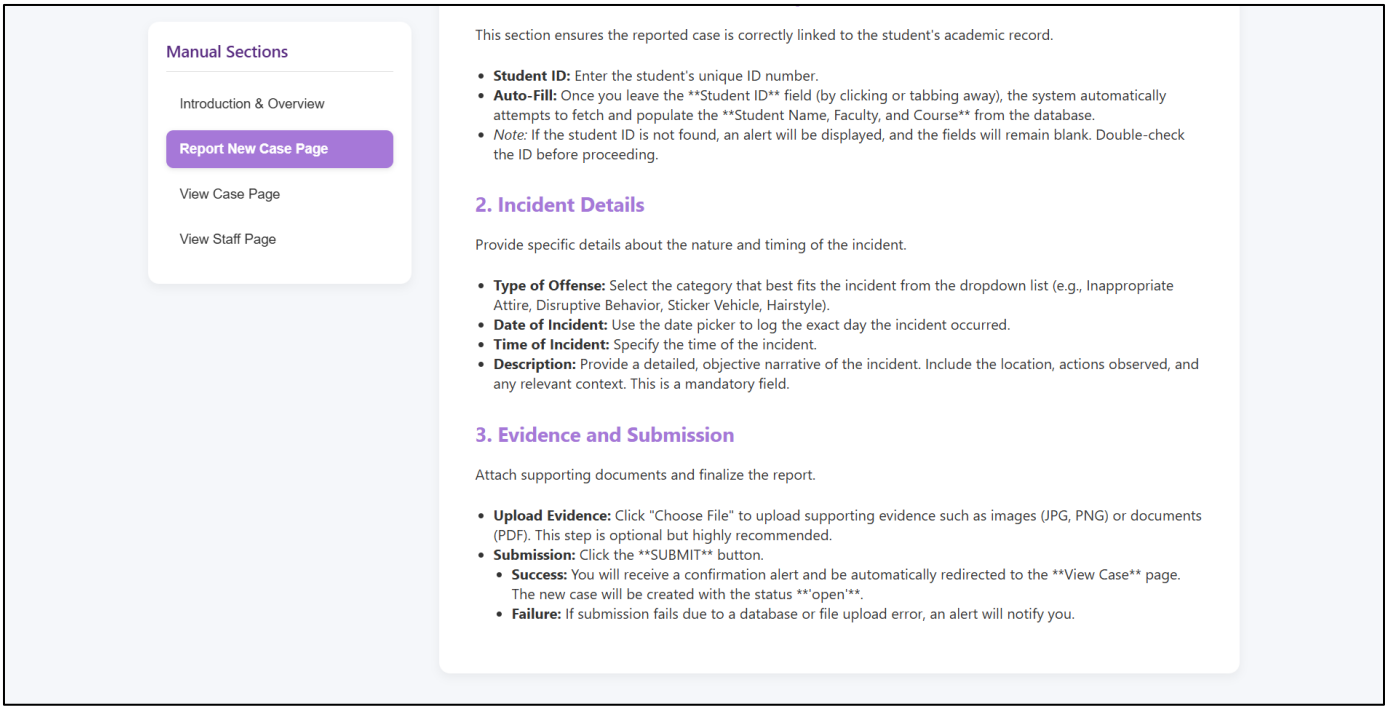

9. Does the system provide accurate and clear information in the disciplinary case records?
Always accurate
Sometimes accurate
Rarely accurate
Not accurate
10. Is the report generation feature clear and easy to understand?
1 2 3 4 5
Strongly Disagree
Strongly Agree
11. Do you have any suggestions or improvements that can make the system better? *
Your answer
Submit
Clear form
Never submit passwords through Google Forms.
This form was created inside of Universiti Poly-Tech Malaysia. - Contact form owner
Does this form look suspicious? Report
Google Forms

Appendix C – User Manual

I. User Manual for Admin







This section ensures the reported case is correctly linked to the student's academic record.

- **Student ID:** Enter the student's unique ID number.
- **Auto-Fill:** Once you leave the **Student ID** field (by clicking or tabbing away), the system automatically attempts to fetch and populate the **Student Name, Faculty, and Course** from the database.
- *Note:* If the student ID is not found, an alert will be displayed, and the fields will remain blank. Double-check the ID before proceeding.

2. Incident Details

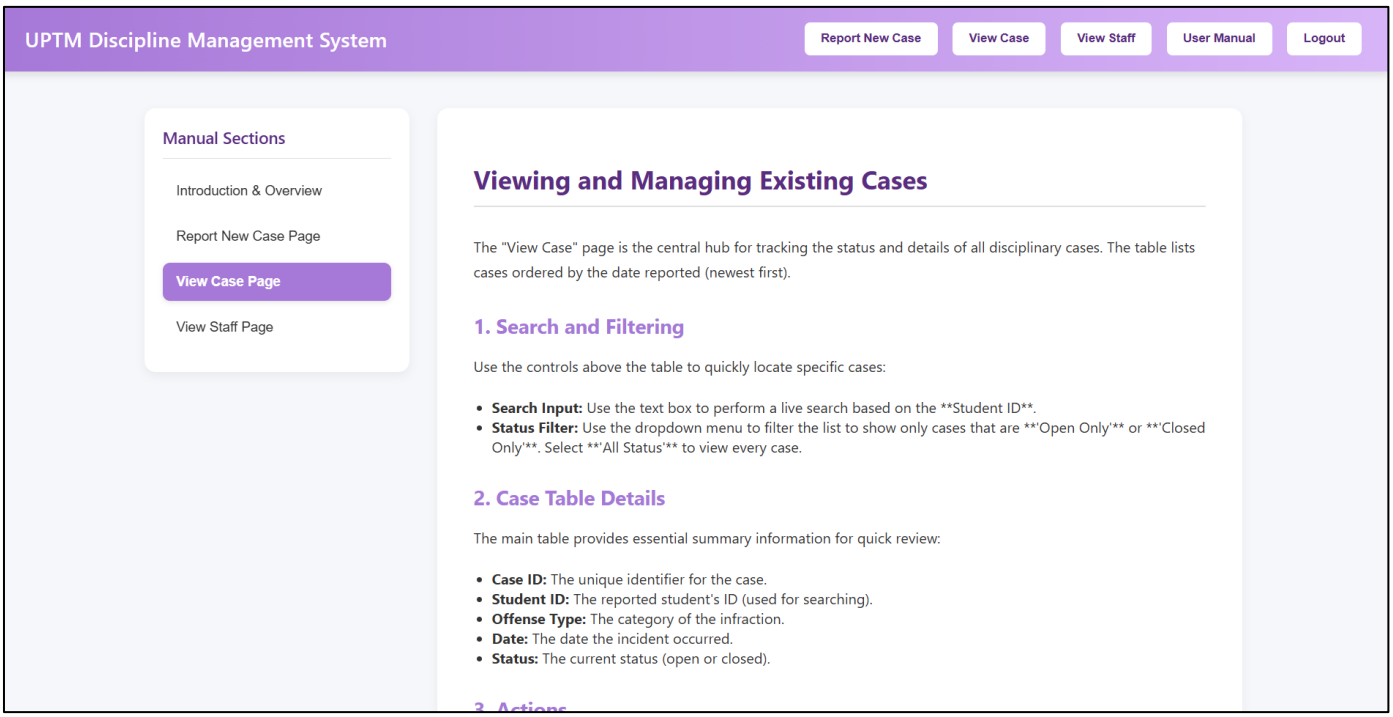
Provide specific details about the nature and timing of the incident.

- **Type of Offense:** Select the category that best fits the incident from the dropdown list (e.g., Inappropriate Attire, Disruptive Behavior, Sticker Vehicle, Hairstyle).
- **Date of Incident:** Use the date picker to log the exact day the incident occurred.
- **Time of Incident:** Specify the time of the incident.
- **Description:** Provide a detailed, objective narrative of the incident. Include the location, actions observed, and any relevant context. This is a mandatory field.

3. Evidence and Submission

Attach supporting documents and finalize the report.

- **Upload Evidence:** Click "Choose File" to upload supporting evidence such as images (JPG, PNG) or documents (PDF). This step is optional but highly recommended.
- **Submission:** Click the **SUBMIT** button.
  - **Success:** You will receive a confirmation alert and be automatically redirected to the **View Case** page. The new case will be created with the status **'open'**.
  - **Failure:** If submission fails due to a database or file upload error, an alert will notify you.



Viewing and Managing Existing Cases

The "View Case" page is the central hub for tracking the status and details of all disciplinary cases. The table lists cases ordered by the date reported (newest first).

1. Search and Filtering

Use the controls above the table to quickly locate specific cases:

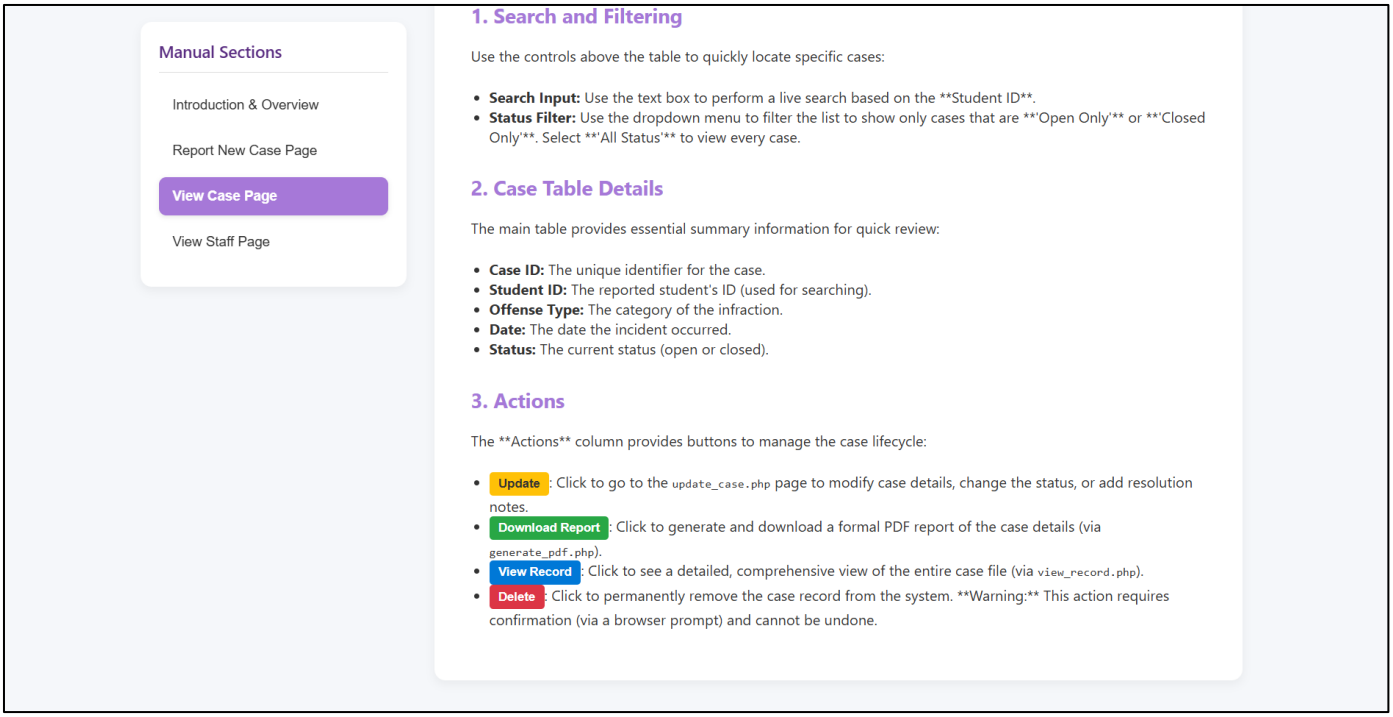
- **Search Input:** Use the text box to perform a live search based on the **Student ID**.
- **Status Filter:** Use the dropdown menu to filter the list to show only cases that are **'Open Only'** or **'Closed Only'**. Select **'All Status'** to view every case.

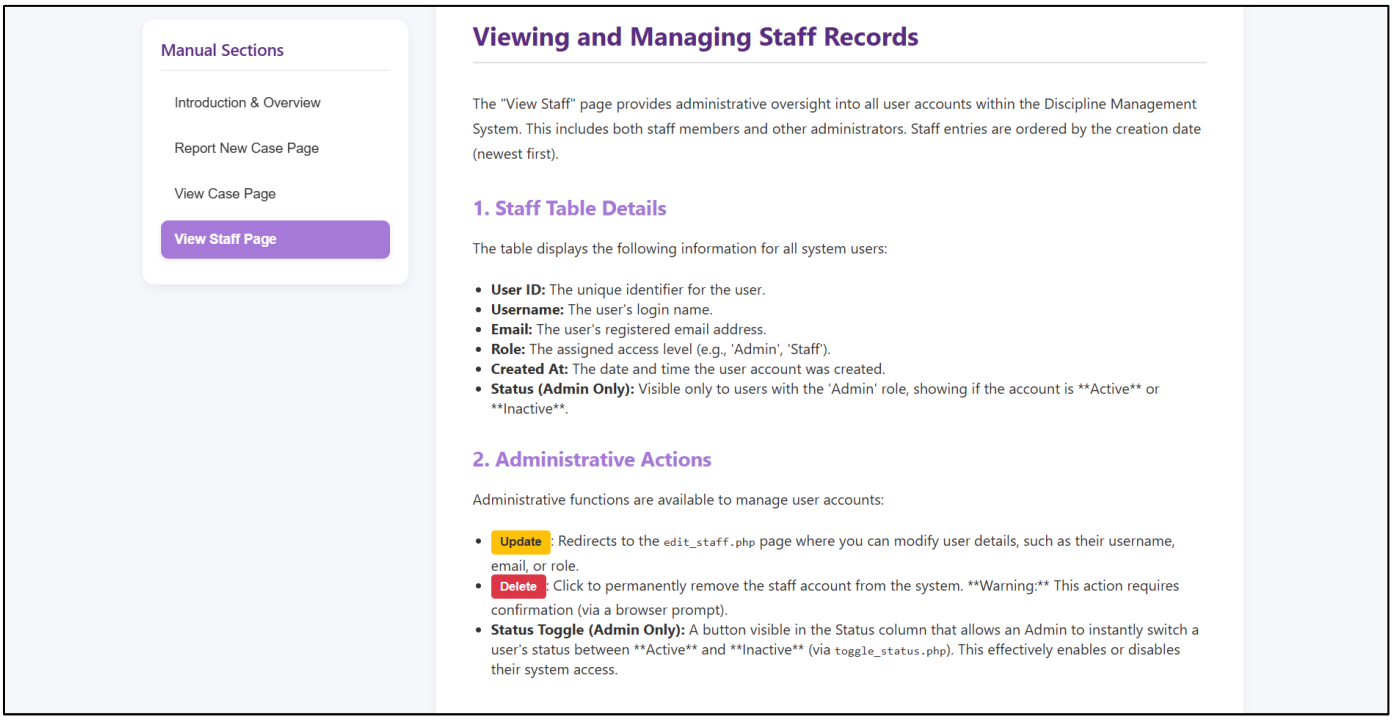
2. Case Table Details

The main table provides essential summary information for quick review:

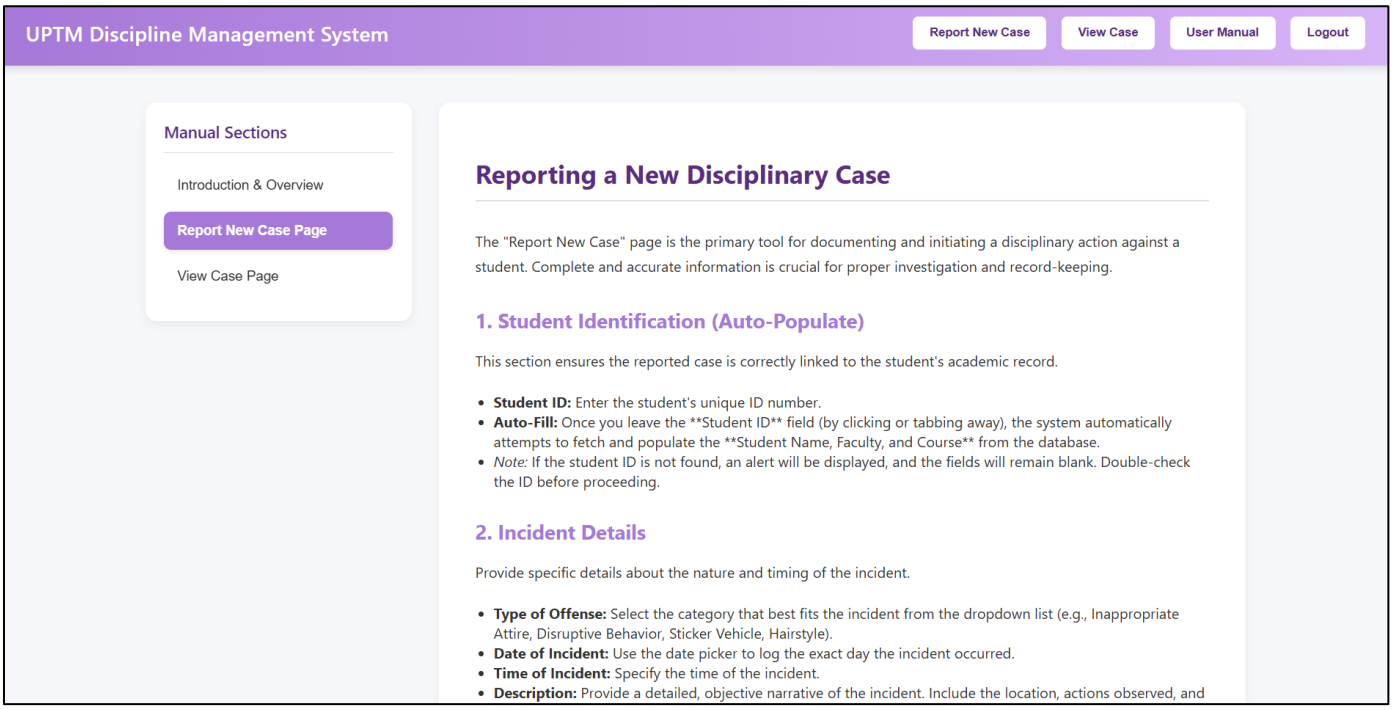
- **Case ID:** The unique identifier for the case.
- **Student ID:** The reported student's ID (used for searching).
- **Offense Type:** The category of the infraction.
- **Date:** The date the incident occurred.
- **Status:** The current status (open or closed).

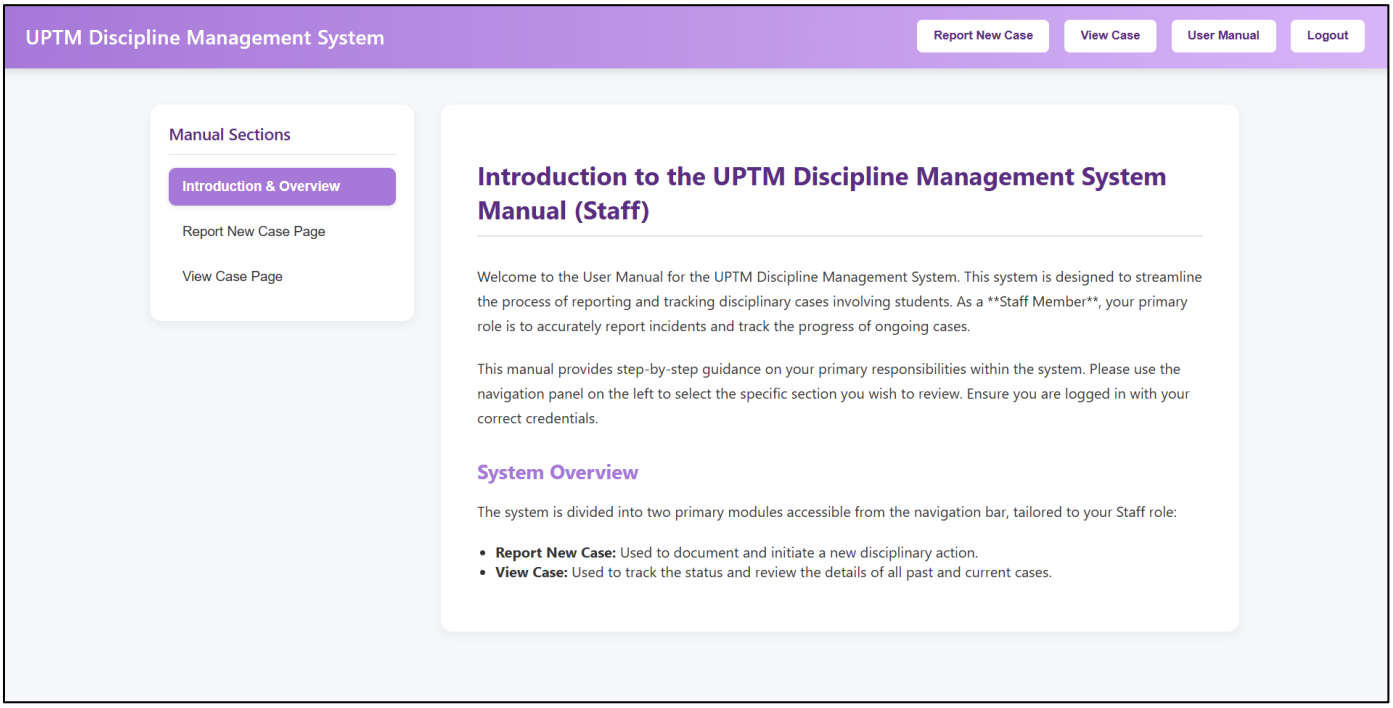
3. Actions

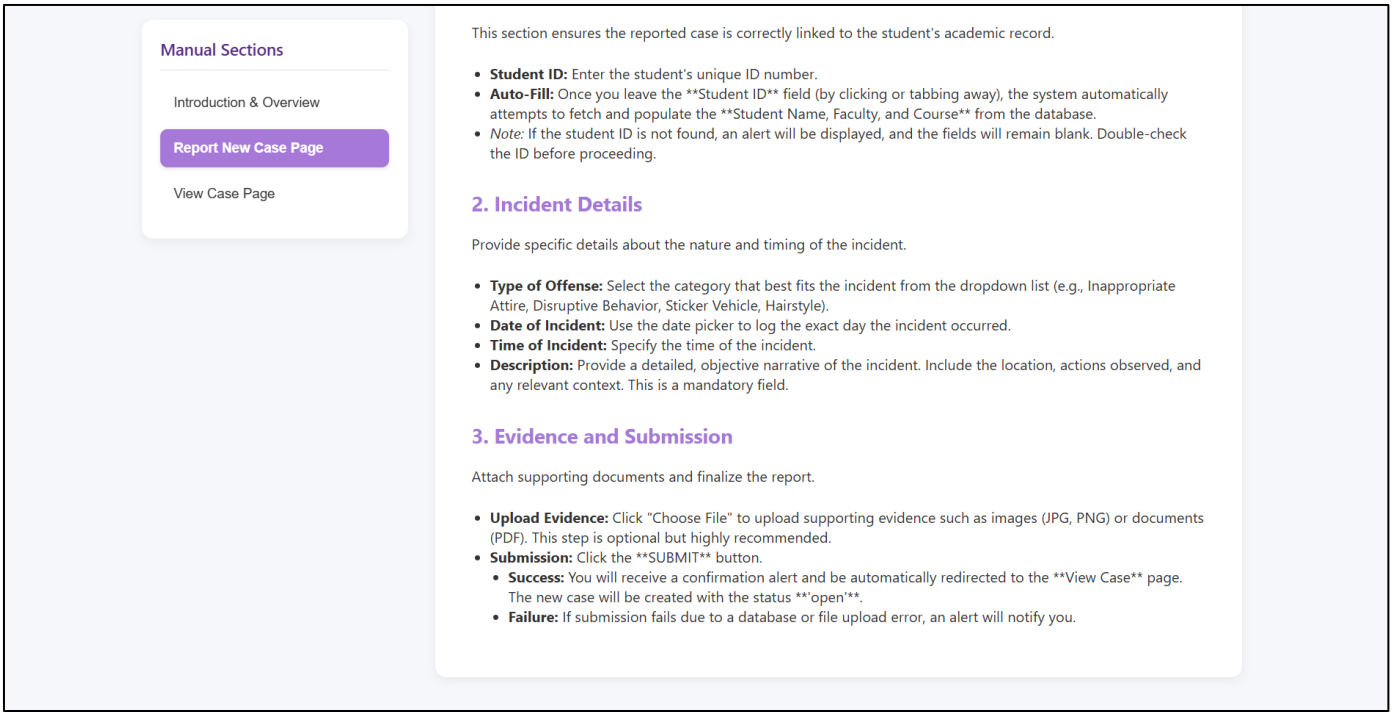

Manual Sections
Introduction & Overview
Report New Case Page
View Case Page
View Staff Page
1. Search and Filtering
Use the controls above the table to quickly locate specific cases:
Search Input: Use the text box to perform a live search based on the **Student ID**.
Status Filter: Use the dropdown menu to filter the list to show only cases that are **'Open Only'** or **'Closed Only'**. Select **'All Status'** to view every case.
2. Case Table Details
The main table provides essential summary information for quick review:
Case ID: The unique identifier for the case.
Student ID: The reported student's ID (used for searching).
Offense Type: The category of the infraction.
Date: The date the incident occurred.
Status: The current status (open or closed).
3. Actions
The **Actions** column provides buttons to manage the case lifecycle:
Update : Click to go to the update_case.php page to modify case details, change the status, or add resolution notes.
Download Report : Click to generate and download a formal PDF report of the case details (via generate_pdf.php).
View Record : Click to see a detailed, comprehensive view of the entire case file (via view_record.php).
Delete : Click to permanently remove the case record from the system. **Warning:** This action requires confirmation (via a browser prompt) and cannot be undone.

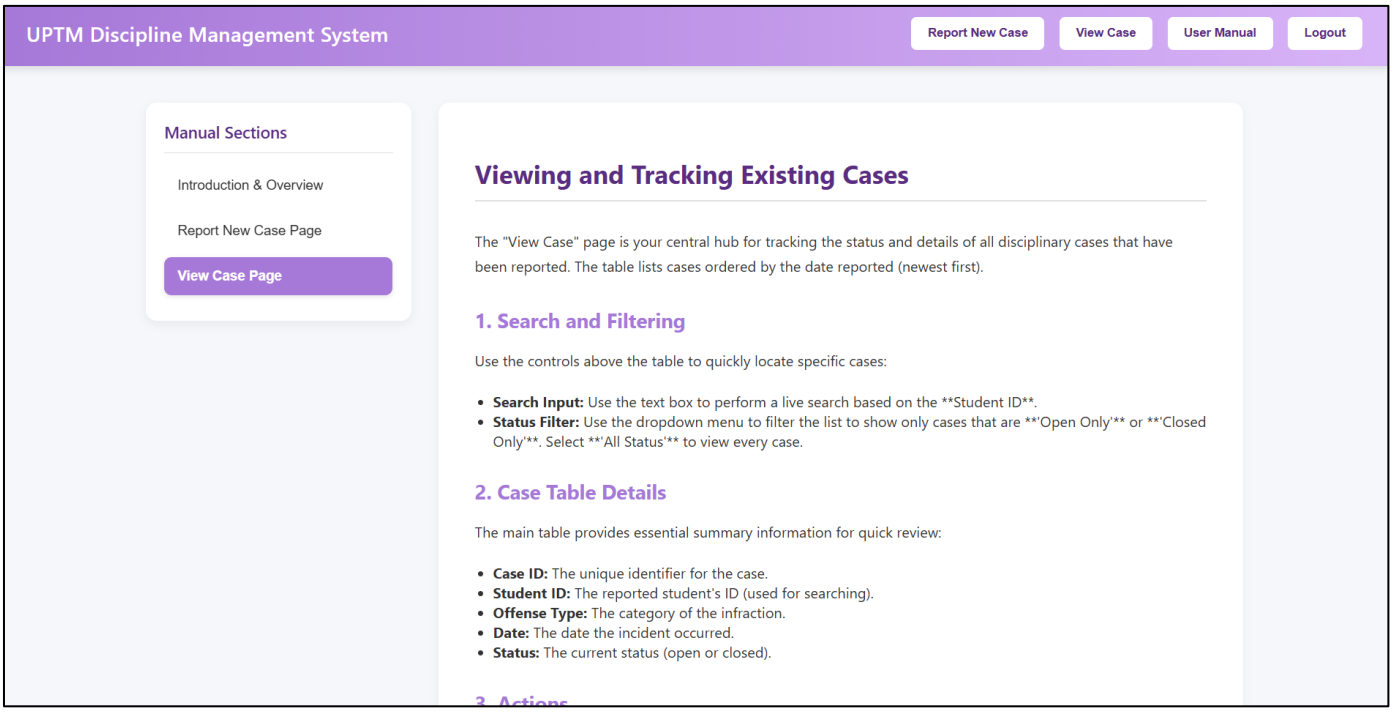

Manual Sections
Introduction & Overview
Report New Case Page
View Case Page
View Staff Page
Viewing and Managing Staff Records
The "View Staff" page provides administrative oversight into all user accounts within the Discipline Management System. This includes both staff members and other administrators. Staff entries are ordered by the creation date (newest first).
1. Staff Table Details
The table displays the following information for all system users:
User ID: The unique identifier for the user.
Username: The user's login name.
Email: The user's registered email address.
Role: The assigned access level (e.g., 'Admin', 'Staff').
Created At: The date and time the user account was created.
Status (Admin Only): Visible only to users with the 'Admin' role, showing if the account is **Active** or **Inactive**.
2. Administrative Actions
Administrative functions are available to manage user accounts:
Update : Redirects to the edit_staff.php page where you can modify user details, such as their username, email, or role.
Delete : Click to permanently remove the staff account from the system. **Warning:** This action requires confirmation (via a browser prompt).
Status Toggle (Admin Only): A button visible in the Status column that allows an Admin to instantly switch a user's status between **Active** and **Inactive** (via toggle_status.php). This effectively enables or disables their system access.

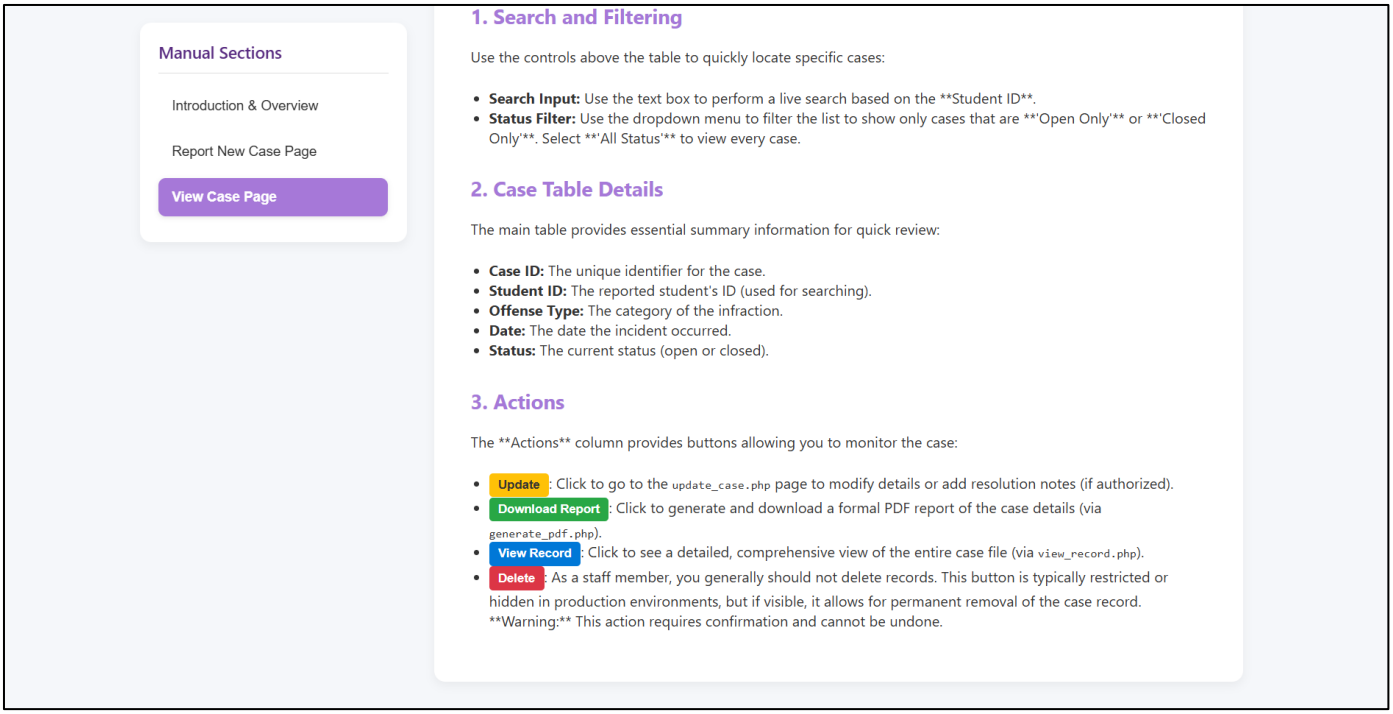
II. User Manual for Staff



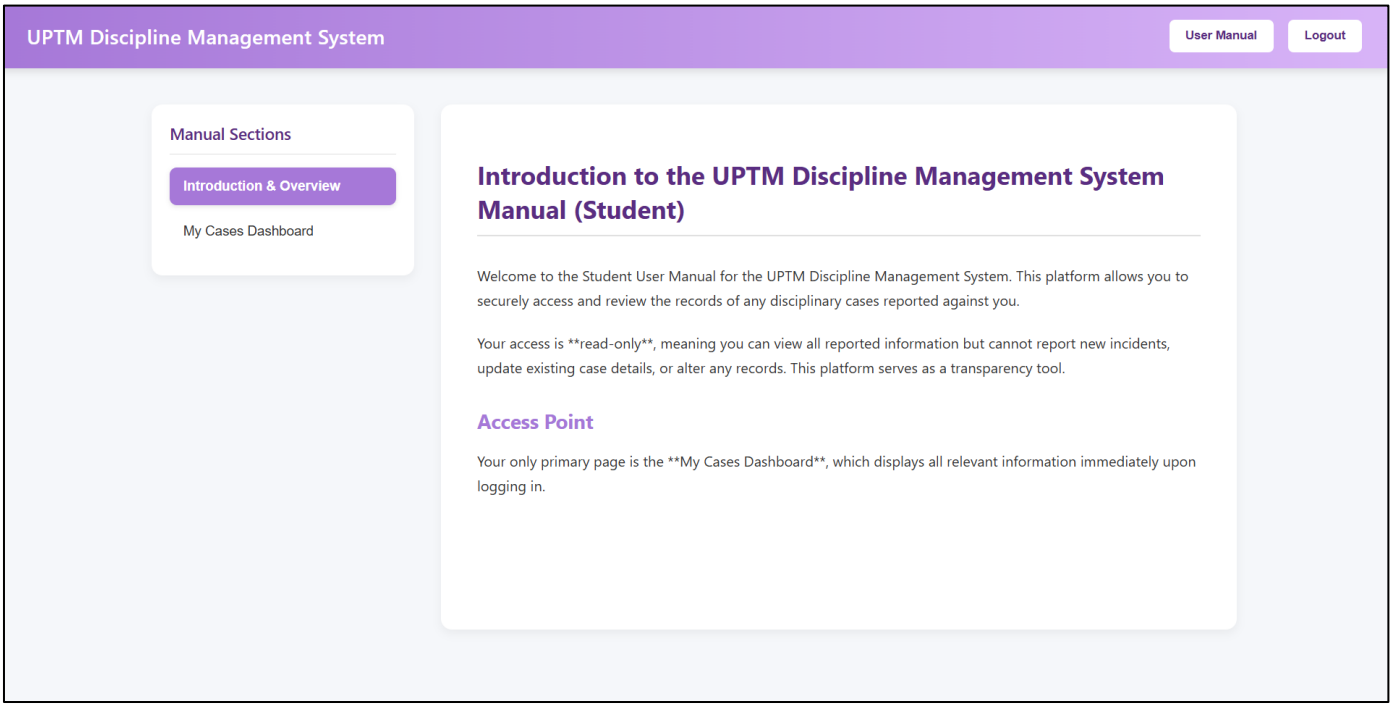


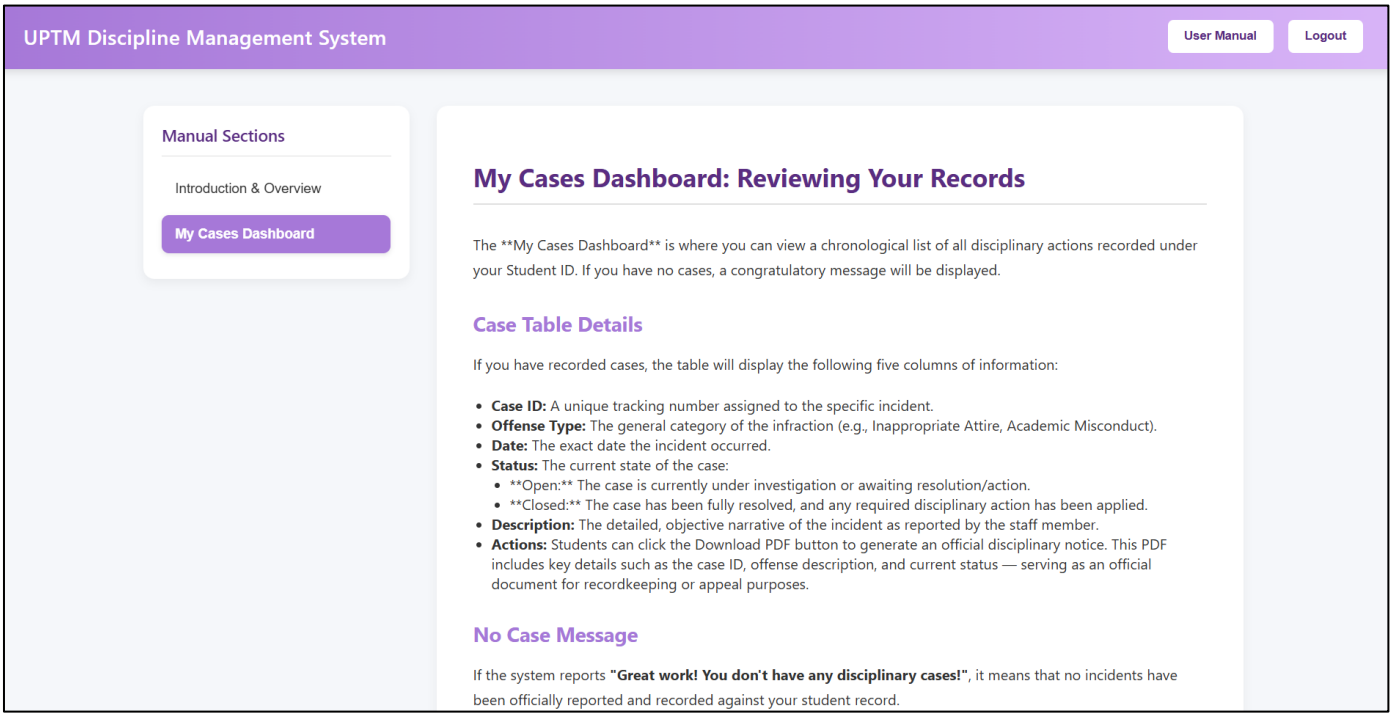

Manual Sections
Introduction & Overview
Report New Case Page
View Case Page
This section ensures the reported case is correctly linked to the student's academic record.
Student ID: Enter the student's unique ID number.
Auto-Fill: Once you leave the **Student ID** field (by clicking or tabbing away), the system automatically attempts to fetch and populate the **Student Name, Faculty, and Course** from the database.
Note: If the student ID is not found, an alert will be displayed, and the fields will remain blank. Double-check the ID before proceeding.
2. Incident Details
Provide specific details about the nature and timing of the incident.
Type of Offense: Select the category that best fits the incident from the dropdown list (e.g., Inappropriate Attire, Disruptive Behavior, Sticker Vehicle, Hairstyle).
Date of Incident: Use the date picker to log the exact day the incident occurred.
Time of Incident: Specify the time of the incident.
Description: Provide a detailed, objective narrative of the incident. Include the location, actions observed, and any relevant context. This is a mandatory field.
3. Evidence and Submission
Attach supporting documents and finalize the report.
Upload Evidence: Click "Choose File" to upload supporting evidence such as images (JPG, PNG) or documents (PDF). This step is optional but highly recommended.
Submission: Click the **SUBMIT** button.
Success: You will receive a confirmation alert and be automatically redirected to the **View Case** page. The new case will be created with the status **'open'**.
Failure: If submission fails due to a database or file upload error, an alert will notify you.


UPTM Discipline Management System
Report New Case
View Case
User Manual
Logout
Manual Sections
Introduction & Overview
Report New Case Page
View Case Page
Viewing and Tracking Existing Cases
The "View Case" page is your central hub for tracking the status and details of all disciplinary cases that have been reported. The table lists cases ordered by the date reported (newest first).
1. Search and Filtering
Use the controls above the table to quickly locate specific cases:
Search Input: Use the text box to perform a live search based on the **Student ID**.
Status Filter: Use the dropdown menu to filter the list to show only cases that are **'Open Only'** or **'Closed Only'**. Select **'All Status'** to view every case.
2. Case Table Details
The main table provides essential summary information for quick review:
Case ID: The unique identifier for the case.
Student ID: The reported student's ID (used for searching).
Offense Type: The category of the infraction.
Date: The date the incident occurred.
Status: The current status (open or closed).


Manual Sections
Introduction & Overview
Report New Case Page
View Case Page
1. Search and Filtering
Use the controls above the table to quickly locate specific cases:
Search Input: Use the text box to perform a live search based on the **Student ID**.
Status Filter: Use the dropdown menu to filter the list to show only cases that are **'Open Only'** or **'Closed Only'**. Select **'All Status'** to view every case.
2. Case Table Details
The main table provides essential summary information for quick review:
Case ID: The unique identifier for the case.
Student ID: The reported student's ID (used for searching).
Offense Type: The category of the infraction.
Date: The date the incident occurred.
Status: The current status (open or closed).
3. Actions
The **Actions** column provides buttons allowing you to monitor the case:
Update : Click to go to the update_case.php page to modify details or add resolution notes (if authorized).
Download Report : Click to generate and download a formal PDF report of the case details (via generate_pdf.php).
View Record : Click to see a detailed, comprehensive view of the entire case file (via view_record.php).
Delete : As a staff member, you generally should not delete records. This button is typically restricted or hidden in production environments, but if visible, it allows for permanent removal of the case record. **Warning:** This action requires confirmation and cannot be undone.

III. User Manual for Student

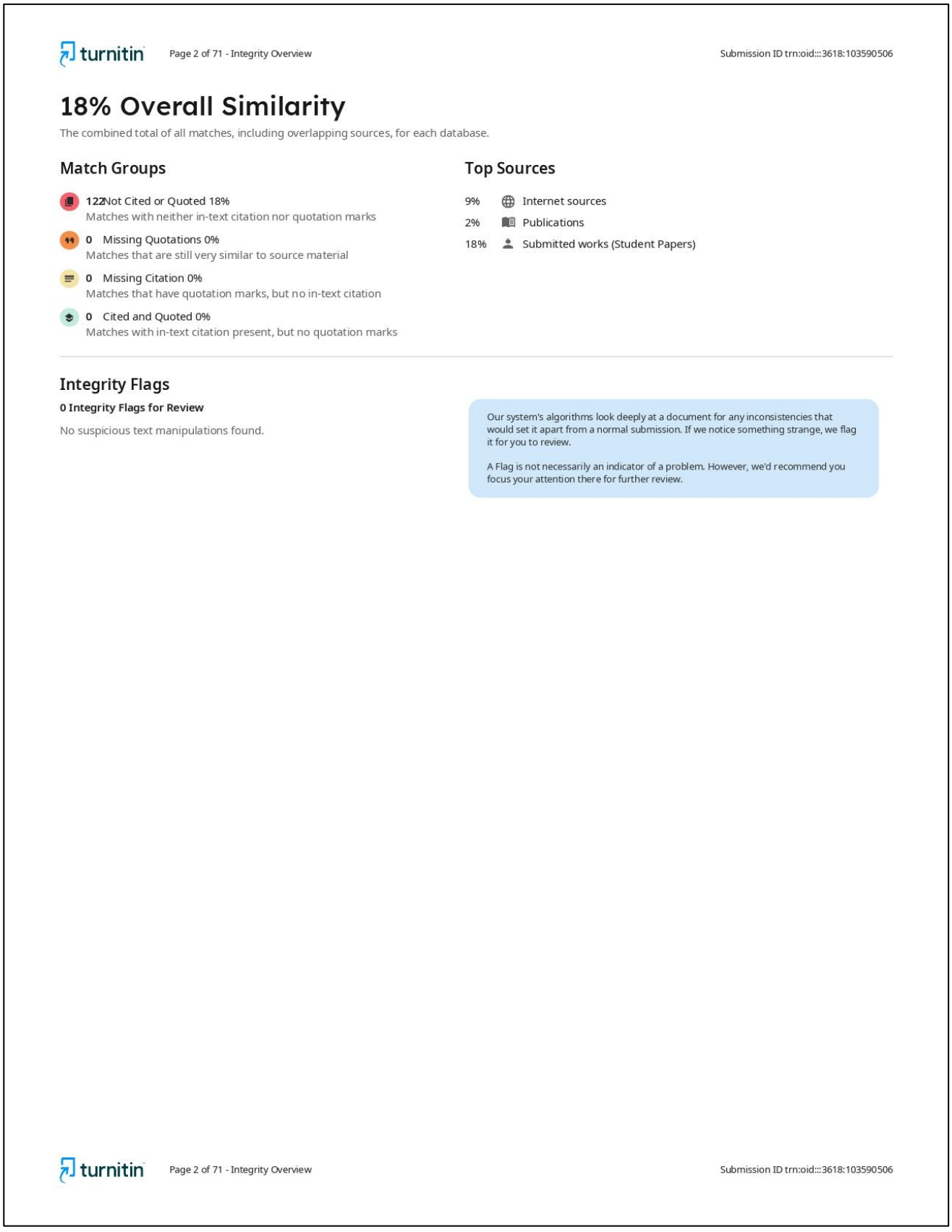





Manual Sections
Introduction & Overview
My Cases Dashboard
The **My Cases Dashboard** is where you can view a chronological list of all disciplinary actions recorded under your Student ID. If you have no cases, a congratulatory message will be displayed.
Case Table Details
If you have recorded cases, the table will display the following five columns of information:
Case ID: A unique tracking number assigned to the specific incident.
Offense Type: The general category of the infraction (e.g., Inappropriate Attire, Academic Misconduct).
Date: The exact date the incident occurred.
Status: The current state of the case:
Open: The case is currently under investigation or awaiting resolution/action.
Closed: The case has been fully resolved, and any required disciplinary action has been applied.
Description: The detailed, objective narrative of the incident as reported by the staff member.
Actions: Students can click the Download PDF button to generate an official disciplinary notice. This PDF includes key details such as the case ID, offense description, and current status — serving as an official document for recordkeeping or appeal purposes.
No Case Message
If the system reports "Great work! You don't have any disciplinary cases!", it means that no incidents have been officially reported and recorded against your student record.
Support
If you believe there is an error in your record or require further clarification on a listed case, please contact the UPTM Administration office directly. The system does not support direct communication or appeal functions.

Appendix D – Turnitin Result

I. Information Security Project 1 (FYP4074)



turnitin Page 2 of 71 - Integrity Overview Submission ID trn:oid:::3618:103590506

18% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- 122 Not Cited or Quoted 18%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

- 9% Internet sources
- 2% Publications
- 18% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

turnitin Page 2 of 71 - Integrity Overview Submission ID trn:oid:::3618:103590506

turnitin Page 3 of 71 - Integrity Overview Submission ID trn:oid:::3618:103590506

Match Groups

- 122 Not Cited or Quoted 18%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

9% Internet sources
2% Publications
18% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	Kolej Universiti Poly-Tech MARA on 2025-04-14 — 2%
2	Submitted works	Kolej Universiti Poly-Tech MARA on 2024-11-26 — <1%
3	Internet	www.coursehero.com — <1%
4	Submitted works	ESoft Metro Campus, Sri Lanka on 2025-04-09 — <1%
5	Submitted works	University of Northumbria at Newcastle on 2025-01-14 — <1%
6	Submitted works	University of Northumbria at Newcastle on 2025-06-16 — <1%
7	Submitted works	Asia Pacific University College of Technology and Innovation (UCTI) on 2024-08-09 — <1%
8	Submitted works	Global Banking Training on 2023-10-10 — <1%
9	Submitted works	National University of Ireland, Galway on 2024-03-29 — <1%
10	Submitted works	West Herts College on 2025-03-03 — <1%

turnitin Page 3 of 71 - Integrity Overview Submission ID trn:oid:::3618:103590506

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

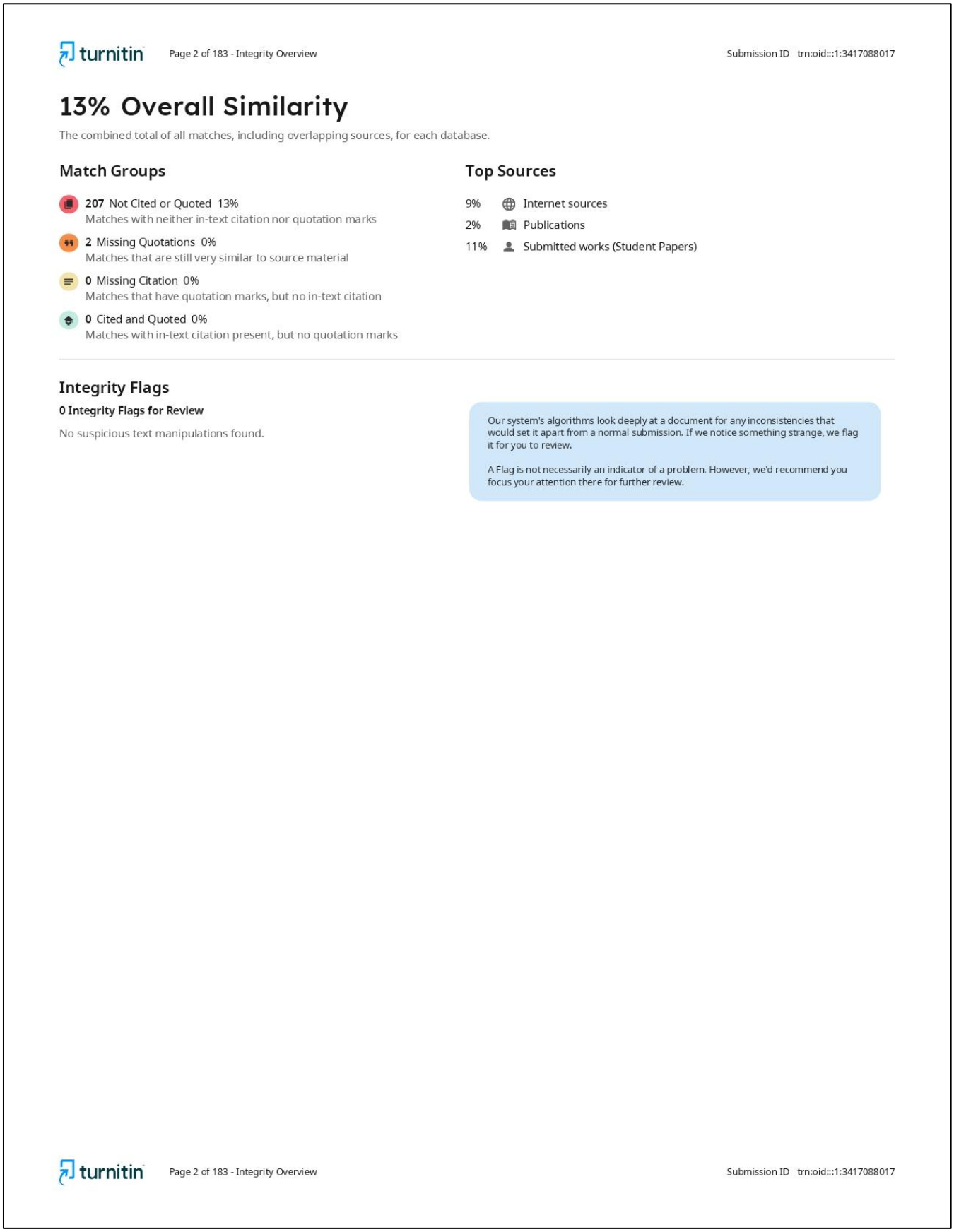
The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

II. Information Security Project 2 (FYP4085)



turnitin Page 2 of 183 - Integrity Overview Submission ID trn:oid:::1:3417088017

13% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

207 Not Cited or Quoted 13%
Matches with neither in-text citation nor quotation marks

2 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

9% Internet sources
2% Publications
11% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

turnitin Page 2 of 183 - Integrity Overview Submission ID trn:oid:::1:3417088017

Match Groups

- **207** Not Cited or Quoted 13%
  Matches with neither in-text citation nor quotation marks
- **2** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

9% Internet sources
2% Publications
11% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
www.interacademycouncil.net		2%
2	Student papers	
Universiti Poly-Tech Malaysia		<1%
3	Internet	
www.coursehero.com		<1%
4	Student papers	
Kolej Universiti Poly-Tech MARA		<1%
5	Student papers	
University of Wales Institute, Cardiff		<1%
6	Student papers	
Global Banking Training		<1%
7	Student papers	
CTI Education Group		<1%
8	Student papers	
University of Westminster		<1%
9	Student papers	
University of Plymouth		<1%
10	Student papers	
University of Greenwich		<1%

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

Appendix E – Log Book

I. Information Security Project 1 (FYP4074)

CT206 / BACHELOR OF IT in CYBER SECURITY (HONOURS)

FACULTY OF COMPUTING & MULTIMEDIA (FCOM)

FINAL YEAR PROJECT O1 FYP4074/FYP4033

LOG BOOK

STUDENT'S NAME: PUTRA AFIQ NASHRIQ BIN ABDUL HADI

ID NO: AM2311015270

SUPERVISOR: PUAN NOR HAFIZA BINTI ABD SAMAD

PROJECT TITLE: SECURE STUDENT DISCIPLINARY RECORD MANAGEMENT SYSTEM

CT206 / BACHELOR OF IT in CYBER SECURITY (HONOURS)

Date/Week		Agenda	Next Agenda	Signature (Supervisor / Coordinator)
(20/05/2025 - 26/05/2025)	1	Project briefing and initial understanding of the problem statement. Preliminary research on existing disciplinary management systems. Drafting of initial project objectives and scope.	Continue in-depth literature review for Chapter 2. Begin defining functional and non-functional requirements.	
(27/05/2025 - 02/06/2025)	2	Completion of Literature Review (Chapter 2). Detailed definition of Functional Requirements (Admin, Staff, Student roles). Detailed definition of Non-Functional Requirements (Security, Usability, Performance, etc.).	Prepare questionnaire for data gathering. Schedule client interview.	
(03/06/2025 - 09/06/2025)	3	Distributed student questionnaire for data collection. Conducted interview with client (Tuan Haji Yahya bin Musa). Began preliminary analysis of gathered data.	Complete data analysis for questionnaire and interview. Start designing Use Case Diagrams.	
(10/06/2025 - 16/06/2025)	4	Completed Data Gathering Analysis (Section 5.2). Designed the initial combined Use Case Diagram for the system. Developed the general high-level flowchart for the disciplinary case management process.	Supervisor meeting to present progress. Address feedback on diagrams and report structure.	
(17/06/2025 - 23/06/2025)	5	Supervisor Meeting conducted; received critical feedback on diagram separation. Redesigned Use Case Diagrams, separating them into Admin, Staff, and Student specific views. Began developing role-specific flowcharts.	Complete all role-specific flowcharts. Update report sections for Use Case Model and Flowchart.	
(24/06/2025 - 30/06/2025)	6	Completed all role-specific flowcharts (Admin User Management, Staff Incident Reporting, Student View Records). Updated Use Case Model (Section 5.3) and Flowchart (Section 5.4) sections in the report. Finalized Functional and Non-Functional Requirement tables.	Review and refine report content for consistency and clarity. Prepare references and logbook.	

CT206 / BACHELOR OF IT in CYBER SECURITY (HONOURS)

(01/07/2025 - 07/07/2025)	7	Final review of the entire report for grammar, formatting, and content consistency. Compiled and formatted the References section. Prepared the Log Book (Appendix).	Final submission of FYP1 report. Prepare for presentation.	

II. Information Security Project 2 (FYP4085)

CT206 / BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY

FACULTY OF COMPUTING & MULTIMEDIA (FCOM)

INFORMATION SECURITY PROJECT 2

(FYP4085)

LOG BOOK

STUDENT'S NAME	:	PUTRA AFIQ NASHRIQ BIN ABDUL HADI
ID NO.	:	AM2311015270
SUPERVISOR	:	PUAN NOR HAFIZA BINTI ABD SAMAD
PROJECT TITLE	:	SECURE STUDENT DISCIPLINARY RECORD MANAGEMENT SYSTEM

CT206 / BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY

Week		Agenda	Next Agenda	Signature (Supervisor / Coordinator)
4 August 2025	1	FYP2 briefing, confirm same client, understand deliverables.	Start system design planning (Chapter 6).	
11 August 2025	2	Plan system structure, features, and design requirements.	Create system wireframes.	
18 August 2025	3	Wireframe creation and submission (19 Aug)	Begin Chapter 6 (Design) writing; brief consultation with supervisor regarding direction of system design.	
25 August 2025	4	Complete and submit Chapter 6 (29 Aug); consultation with supervisor about design clarity.	Start system development for implementation.	
1 September 2025	5	System development (login, roles, CRUD modules).	Continue implementation work.	
8 September 2025	6	Implementation progress (case module, UI, validation).	Prepare for Chapter 7 Implementation reporting.	
MID-TERM BREAK				
22 September 2025	7	Continue system development and internal testing.	Draft Chapter 7.	
29 September 2025	8	Chapter 7 report progress submission.	Write full Chapter 7 (Implementation).	
6 October 2025	9	Chapter 7 writing and update based on development.	Start Chapter 8 (Testing).	
13 October 2025	10	Write Chapter 8 testing section and collect test results.	Proceed to Chapter 9.	

CT206 / BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY

20 October 2025	11	Write Chapter 9 (Project Management).	Complete Chapter 10.	
27 October 2025	12	Write Chapter 10 (Conclusion & Future Work).	Finalize system, create Google Form questionnaire for UAT and prepare for demo.	
3 November 2025	13	System refinement; created Google Form questionnaire for UAT; Demo to supervisor and client (6 Nov).	Prepare final report & presentation.	
10 November 2025	14	Final report submission and FYP presentation (13 Nov).	(End of FYP2)	

References

AltexSoft (2023). *Functional and Non-functional Requirements: Specification an*. [online] AltexSoft. Available at: https://www.altexsoft.com/blog/functional-and-non-functional-requirements-specification-and-types/.

Alutbi, M. (2020). *Work Breakdown Structure (WBS)*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/342163727_WORK_BREAKDOWN_STRUCTURE_WBS.

Anandhan (2023). *Is your Laravel application secure? Exploring common security pitfalls and their solutions*. [online] Web and mobile app development company -. Available at: https://mallow-tech.com/blog/is-your-laravel-application-secure-exploring-common-security-pitfalls-and-their-solutions/?utm_source=chatgpt.com [Accessed 5 Jul. 2025].

Aquino, E., de Saqui-Sannes, P. and Vingerhoeds, R. (2020). A Methodological Assistant for Use Case Diagrams. *Proceedings of the 8th International Conference on Model-Driven Engineering and Software Development*. [online] doi:https://doi.org/10.5220/0008938002270236.

Arias, D. (2019). *Hashing Passwords: One-Way Road to Security*. [online] Auth0 - Blog. Available at: https://auth0.com/blog/hashing-passwords-one-way-road-to-security/.

Aspinall, D. (n.d.). *Secure Programming Lecture 10: Web Application Security I (OWASP, HTTP)*. [online] Available at: https://opencourse.inf.ed.ac.uk/sites/default/files/https/opencourse.inf.ed.ac.uk/sp/2024/10-webapp.pdf [Accessed 18 Nov. 2025].

Azameti, M. S. K., & Adjei, E. (2013). *Challenges in Academic Records Management in Tertiary Institutions in Ghana.* [online] International Journal of Scientific Research in Education, 6(3), 287–296. Available at: https://www.ijsre.com.ng/assets/vol.%2C-6_3_-azameti---adjei.pdf?utm_source=chatgpt.com.

Balsamiq.com. (2025). *What is a wireframe? A guide for non-designers*. [online] Available at: https://balsamiq.com/blog/what-are-wireframes/.

Bhat, A. (2020). *Data collection methods: Definition, examples and sources*. [online] QuestionPro. Available at: https://www.questionpro.com/blog/data-collection-methods/.

Bhupendra (2024). *Password Hashing using bcrypt - Bhupendra - Medium*. [online] Medium. Available at: https://medium.com/@bhupendra_Maurya/password-hashing-using-bcrypt-e36f5c655e09.

Blackduck (2023). *What Is Cross-Site Request Forgery (CSRF) and How Does It Work? | Black Duck*. [online] blackduck.com. Available at: https://www.blackduck.com/glossary/what-is-csrf.html.

Blum, D. (2020). *Security Reference Architecture Authors*. [online] Available at: https://techvisionresearch.com/wp-content/uploads/2020/12/Security-Reference-Architecture-Excerpt-20201129-Final.pdf.

BrowserStack. (n.d.). *Differences Between Functional and Non-functional Testing*. [online] Available at: https://www.browserstack.com/guide/functional-vs-non-functional-testing.

Brush, K. and Silverthorne, V. (2022). *What is Agile Software Development (Agile Methodologies)?* [online] TechTarget. Available at: https://www.techtarget.com/searchsoftwarequality/definition/agile-software-development.

Cacoo Staff (2021). *How a UML use case diagram can benefit any process*. [online] Nulab. Available at: https://nulab.com/learn/software-development/how-a-uml-use-case-diagram-can-benefit-any-process/.

Chapter 6. Data-Flow Diagrams. (n.d.). Available at: https://www.cs.uct.ac.za/mit_notes/software/pdfs/Chp06.pdf.

Chia, A. (2024). *User Acceptance Testing (UAT): Definition, Types & Best Practices | Splunk*. [online] Splunk. Available at: https://www.splunk.com/en_us/blog/learn/user-acceptance-testing-uat.html.

Cloudflare (2024). *How to prevent SQL injection*. [online] Cloudflare.com. Available at: https://www.cloudflare.com/learning/security/threats/how-to-prevent-sql-injection/.

dataedo.com. (n.d.). *6 Useful SQL Server Data Dictionary Queries Every DBA Should Have - Dataedo Blog*. [online] Available at: https://dataedo.com/blog/useful-sql-server-data-dictionary-queries-every-dba-should-have.

dottotech (2022). *How to set up Two-Factor Authentication (2FA) for all your accounts*. [online] YouTube. Available at: https://www.youtube.com/watch?v=hlpoc3C1kWM [Accessed 6 Feb. 2025].

draw.io (2025). *Flowchart Maker & Online Diagram Software*. [online] app.diagrams.net. Available at: https://app.diagrams.net/.

EBSCO Information Services, Inc. | www.ebsco.com. (2021). *Work Breakdown Structure | EBSCO*. [online] Available at: https://www.ebsco.com/research-starters/business-and-management/work-breakdown-structure.

Educationhorizons.com. (2023). *Student Record Management Systems for Schools*. [online] Available at: https://www.educationhorizons.com/solutions/zunia/student-record-management-systems-for-schools.

Far, N. (2020). *How to implement password recovery securely in PHP*. [online] Medium. Available at: https://itnext.io/how-to-implement-password-recovery-securely-in-php-db2275ab3560.

Figma (2023). *What is UI Design? | Figma*. [online] Figma. Available at: https://www.figma.com/resource-library/what-is-ui-design/.

Fortinet (2025). *What Is Two-factor Authentication (2FA)?* [online] Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary/two-factor-authentication.

frontegg (2022). *Authentication: Methods, Protocols, and Strategies*. [online] Frontegg. Available at: https://frontegg.com/blog/authentication.

GeeksforGeeks (2025). *Introduction of ER Model*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/dbms/introduction-of-er-model/.

GeeksforGeeks (2023). *Use Case Diagram Unified Modeling Language (UML)*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/system-design/use-case-diagram/.

Graham, M., Falkner, K., Szabo, C. and Yarom, Y. (n.d.). *Security Architecture Framework for Enterprises*. [online] Available at: https://yuval.yarom.org/pdfs/GrahamFSY21.pdf.

hep@um.edu.my (2024). *Student Affairs Department*. [online] Um.edu.my. Available at: https://hep.um.edu.my/disciplinary [Accessed 5 Jul. 2025].

IBM (2025). *Integration testing*. [online] Ibm.com. Available at: https://www.ibm.com/think/topics/integration-testing.

Iliya (2024). *Enhancing PHP Session Security: Best Practices and Solutions*. [online] Medium. Available at: https://medium.com/@bazlyankov/enhancing-php-session-security-best-practices-and-solutions-c8d3ef22632d.

Imperva (2024). *What is SQL Injection | SQLI Attack Example & Prevention Methods | Imperva*. [online] Imperva. Available at: https://www.imperva.com/learn/application-security/sql-injection-sqli/.

Indeed Career Guide. (n.d.). *How To Make a Gantt Chart in Word in 5 Steps (Plus Tips)*. [online] Available at: https://www.indeed.com/career-advice/career-development/making-a-gantt-chart-in-word.

Indeed, Career Guide. (n.d.). *Systems Analyst Interview Questions With Example Answers*. [online] Available at: https://www.indeed.com/career-advice/interviewing/systems-analyst-interview-questions.

iSAMS. (n.d.). *School Management Information System*. [online] Available at: https://www.isams.com/.

Kintone. (2017). Kintone - An all-in-one workplace platform that allows highly collaborative teams to build, share, and automate custom workflows and processes for data-driven results. [online] Available at: https://www.kintone.com/en-sea/.

Laoyan, S. (2025). *What is agile methodology? (A beginner's guide)*. [online] Asana. Available at: https://asana.com/resources/agile-methodology.

Laravel (2015). *Laravel - The PHP Framework For Web Artisans*. [online] Laravel.com. Available at: https://laravel.com/.

Lenaerts-Bergmans, B. (2022). *What is a SQL Injection Attack?* | *CrowdStrike*. [online] Crowdstrike.com. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/sql-injection-attack/.

Llego, M.A. (2023). *The Ultimate Gantt Chart Guide for Academic Research: Streamlining Your Timetable and Increasing Productivity*. [online] TeacherPH. Available at: https://www.teacherph.com/ultimate-gantt-chart-guide-academic-research/#google_vignette.

Lindemulder, G. and Kosinski, M. (2024). *What is role-based access control (RBAC)?* [online] IBM. Available at: https://www.ibm.com/think/topics/rbac.

Liu, Y. and Stoller, S. (n.d.). *Role-Based Access Control: A Simplified Specification* *. [online] Available at: https://www3.cs.stonybrook.edu/~liu/papers/RBAC-TR05.pdf.

Lucidchart (2019). *UML Use Case Diagram Tutorial*. [online] Lucidchart.com. Available at: https://www.lucidchart.com/pages/uml-use-case-diagram.

Manchester.ac.uk. (2025). *Discipline Case Studies | Advice and response | StaffNet | The University of Manchester*. [online] Available at: https://www.staffnet.manchester.ac.uk/adviceandresponse/resources/discipline-case-studies/ [Accessed 5 Jul. 2025].

MDN Web Docs. (2025). *Getting started with CSS - Learn web development | MDN*. [online] Available at: https://developer.mozilla.org/en-US/docs/Learn_web_development/Core/Styling_basics/Getting_started.

Microsoft (2024). *Microsoft Cybersecurity Reference Architectures (MCRA)*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/security/adoption/mcra.

Microsoft (2025). *Visual Studio Code*. [online] Visualstudio.com. Available at: https://code.visualstudio.com/.

MyGovernment (2024). *MyGOV - The Government of Malaysia's Official Portal*. [online] www.malaysia.gov.my. Available at: https://www.malaysia.gov.my/portal/content/654.

Nguyen, T. (2023). *Complete Guide to Software Development Requirements*. [online] Trusted IT Outsourcing Provider. Available at: https://rikkeisoft.com/blog/software-development-requirements/.

NIH (2020). *Data Gathering and Analysis*. [online] Office of Human Resources. Available at: https://hr.nih.gov/working-nih/competencies/competencies-dictionary/data-gathering-and-analysis.

Nishadha (2022). *Use case diagram tutorial (guide with examples) | creately*. [online] creately.com. Available at: https://creately.com/guides/use-case-diagram-tutorial/.

Oracle.com. (2025). *Understanding Login Authentication*. [online] Available at: https://docs.oracle.com/javaee/1.4/tutorial/doc/Security5.html.

Orca Security. (2025). *RBAC (Role-Based Access Control)*. [online] Available at: https://orca.security/glossary/rbac-role-based-access-control/ [Accessed 18 Nov. 2025].

OWASP (2017). *Authentication · OWASP Cheat Sheet Series*. [online] Owasp.org. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html.

OWASP (2020). *Cross Site Scripting (XSS) | OWASP*. [online] Owasp.org. Available at: https://owasp.org/www-community/attacks/xss/.

OWASP (2025). *SQL Injection Prevention · OWASP Cheat Sheet Series*. [online] Owasp.org. Available at: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.

PCMAG. (n.d.). *Windows 11 Home vs. Pro: What Are the Differences?* [online] Available at: https://www.pcmag.com/comparisons/windows-11-home-vs-pro.

PHP (2019). *PHP: Prepared Statements - Manual*. [online] Php.net. Available at: https://www.php.net/manual/en/mysqli.quickstart.prepared-statements.php.

PortSwigger (2019). *What is CSRF (Cross-site request forgery)? Tutorial & Examples*. [online] Portswigger.net. Available at: https://portswigger.net/web-security/csrf.

Pym, D.V. (1987). *Risk Management | PMI*. [online] www.pmi.org. Available at: https://www.pmi.org/learning/library/risk-management-9096.

PythonBasics (2021). *What is Flask Python - Python Tutorial*. [online] pythonbasics.org. Available at: https://pythonbasics.org/what-is-flask-python/.

Ramani, Y., Tilala, U., Dholariya, S. and Soni, S. (2025). Student Record System Project. © *2025 IJRTI* |, [online] 10, p.470. Available at: https://ijrti.org/papers/IJRTI2503168.pdf.

Reddit.com. (2022). *Reddit - The heart of the internet*. [online] Available at: https://www.reddit.com/r/Backend/comments/x6g7an/laravel_vs_flask/.

Rework.com. (2025). *Creating a Gantt Chart for Your Research Project Proposal*. [online] Available at: https://resources.rework.com/libraries/guides/creating-a-gantt-chart-for-your-research-project-proposal [Accessed 18 Nov. 2025].

runestone.academy. (n.d.). *2.2. Entity-relationship diagrams — A Practical Introduction to Databases*. [online] Available at: https://runestone.academy/ns/books/published/practical_db/PART2_DATA_MODELING/02-ERD/ERD.html.

schoolday (2024). *Safeguarding Student Data - SchoolDay*. [online] SchoolDay. Available at: https://www.schoolday.com/safeguarding-student-data-understanding-the-importance-of-privacy-in-the-digital-age/.

Schwartz, B. (2025). *The Risk Management Process in Project Management*. [online] ProjectManager. Available at: https://www.projectmanager.com/blog/risk-management-process-steps.

Sebastian, M., Kwame Azameti and Adjei, E. (2013). Challenges in Academic Records Management in Tertiary Institutions in Ghana. [online] 6(3), pp.287–296. Available at: https://www.researchgate.net/publication/277713712_Challenges_in_Academic_Records_Management_in_Tertiary_Institutions_in_Ghana.

Secoda.co. (2024). *What Are the Common Methods for Data Gathering? | Secoda*. [online] Available at: https://www.secoda.co/learn/what-are-the-common-methods-for-data-gathering.

Session (2025). *ThreatNG Security*. [online] ThreatNG Security. Available at: https://www.threatngsecurity.com/glossary/session-hardening-recommendations [Accessed 18 Nov. 2025].

Smartdraw.com. (2022). *Flowchart - Process Flow Charts, Templates, How To, and More*. [online] Available at: https://www.smartdraw.com/flowchart/?srsltid=AfmBOoqRZumHdh5_Hx7_5J5JsDGAEY6yAzzrQ3REvxXGakXDbAlO8Kw [Accessed 5 Jul. 2025].

Smith, R.S. (2024). *Student data privacy problems and challenges to be aware of in 2024*. [online] Novatia.com. Available at: https://www.novatia.com/blog/student-data-privacy-problems-and-challenges-to-be-aware-of-in-2024.

Stack Overflow. (n.d.). *Generating data dictionary for SQL Server database*. [online] Available at: https://stackoverflow.com/questions/6487885/generating-data-dictionary-for-sql-server-database.

Stack Overflow. (n.d.). *How to view an HTML file in the browser with Visual Studio Code*. [online] Available at: https://stackoverflow.com/questions/30039512/how-to-view-an-html-file-in-the-browser-with-visual-studio-code.

Surianom Miskam, Nawal Sholehuddin, Farah Mohd Shahwahid, Nurhafiza, T. and Mansor, N. (2023). Data Privacy Practices of Private Higher Education Institutions in Malaysia: A Preliminary Study. *Deleted Journal*, pp.88–99. doi:https://doi.org/10.53840/myjict8-2-99.

Systems Librarian (2024). *Systems Librarian -- Computers in Libraries / Information Today by Marshall Breeding*. [online] Librarytechnology.org. Available at: https://librarytechnology.org/systemslibrarian/ [Accessed 6 Jul. 2025].

Team, L. (2024). *Mastering Secure Access: The Ultimate Guide to Login Authentication*. [online] LoginRadius. Available at: https://www.loginradius.com/blog/identity/what-is-login-authentication.

Ukmsl.com. (2025). *What is student case management software and why you need it*. [online] Available at: https://www.ukmsl.com/news/article/msl/What-is-student-case-management-software-and-why-you-need-it/ [Accessed 5 Jul. 2025].

Universiti Poly-Tech Malaysia (2024) Buku peraturan dan panduan tatatertib pelajar UPTM. Available at: https://www.uptm.edu.my (Accessed: 5 July 2025).

University of Minnesota (2022). *Agile methodology: Advantages and disadvantages*. [online] University of Minnesota. Available at: https://ccaps.umn.edu/story/agile-methodology-advantages-and-disadvantages.

Uxmatters.com. (2023). *How Developing Use Cases Helps in Designing User Interactions :: UXmatters*. [online] Available at: https://www.uxmatters.com/mt/archives/2023/11/how-developing-use-cases-helps-in-designing-user-interactions.php.

Veracode. (2025). *What is Cross-Site Scripting? XSS Cheat Sheet*. [online] Available at: https://www.veracode.com/security/xss/.

Visual Paradigm (2019). *Flowchart Tutorial (with Symbols, Guide and Examples)*. [online] Visual-paradigm.com. Available at: https://www.visual-paradigm.com/tutorials/flowchart-tutorial/.

W3schools.com. (n.d.). *Introduction to Python*. [online] Available at: https://www.w3schools.com/python/python_intro.asp.

Wikipedia Contributors (2025). *SQL injection*. Wikipedia.

www.magicslides.app. (2020). *How to use Google forms to collect data*. [online] Available at: https://www.magicslides.app/blog/how-to-use-google-forms-to-collect-data.

www.microsoft.com. (n.d.). *What is two-factor authentication (2FA)? | Microsoft Security*. [online] Available at: https://www.microsoft.com/en-my/security/business/security-101/what-is-two-factor-authentication-2fa.

www.softkraft.co. (n.d.). *How to Write Software Requirements - 12 Do's and Don'ts*. [online] Available at: https://www.softkraft.co/how-to-write-software-requirements/.