SOFTWARE REQUIREMENT SPECIFICATION
FOR

POLICE COMPLAINT MANAGEMENT SYSTEM (PCMS)

Version: 1.0

TABLE OF CONTENT

1.0 Introduction

1.1 Purpose

This document establishes the operational and technical specifications for the Police Complaint Management System .This SRS covers the complete system deployment including the front-end web interface, back-end database management,security modules, and the reporting capabilities.The scope encompasses initial system launch supporting citizen complaint submission, officer case management, administrative oversight and the comprehensive analysis The motive of this document is to serve as a comprehensive guide for the stakeholders, developers, testers and other project participants, detailing the goals of the system, features and constraints.

The PCMS(Police Complaint Management System) intends to modernize and streamline the process of lodging, tracking and managing police complaints within Fiji's law enforcement framework. This SRS addresses the entire system , covering all major modules, including submission of complaints(by citizens and visitors to the country), complaint handling(by officials and administrators), Role based dashboard, and reports and analytics.The scope of this SRS includes the initial complete launch of the PCMS(Police Complaint Management System), which includes both the front-end web interface and the back-end database management system, in addition to the incorporation of pertinent security and reporting tools.

1.2 Document Conventions

Typography: Main content uses 12-point Times New Roman font with emphasized headings for primary sections

Requirement Labels: Each requirement shall be uniquely be identified using the format REQ-[Section]-[Number] e.g. (for instance, REQ-4.1-01 for first requirement in section 4.1)

Priority levels:

- High(H) – Must be implemented in the initial release
- Medium(M) – Important, yet it may be included in later updates

- Low(L) – Optional or enhancement features that may be implemented if time persists.

Status Indicators

- [IMPLEMENTED]:Requirement fully developed
- [PENDING]:Requirement identified but not yet developed
- [TBD]: To be determined- requires further analysis

Terminology:

- Citizen: A registered user submitting complaints
- Guest: An unregistered individual submitting complaint.
- Officer: Authorized personnel in the law enforcement sector
- Admin(Administrators) : A system admin responsible for managing users and the system configurations and functionalities

1.3 Intended Audience and Reading Suggestions

This document serves multiple stakeholder groups:

- Software Engineers – for understanding technical specifications and system capabilities
- Project managers – for tracking the scope, deliverables and the timelines of the project.
- Law Enforcement Authorities- For validating operations needs and compliance
- Testers/QA(Quality Assurance) Engineers – For developing and implementing test cases
- Documentation Writers-For preparing user manuals and support materials.

Reading Recommendations:
Reading Sequence:

1. Begin with Section 1 (Introduction) for system overview and scope
2. Examine Section 2 for comprehensive system architecture overview
3. Software engineers: Concentrate on Sections 3-4 for implementation details
4. Testers: Utilize Section 4 functional requirements for test case development
5. Consult appendices for supporting information and definitions.

1.4 Product Scope

The police complaint management system is an online web based platform designed to improve transparency, efficiency, and accessibility in the management of police complaints. The system enables citizens, visitors and other stakeholders to submit complaints online , track their progress, and obtain timely notifications.

Key objectives:

- Minimize dependence on manual, paper-based complaint logging.
- Enhancing the processing time through automated workflows
- Provide secure , role based access to safeguard sensitive information.
- Generate accurate reports for better decision -making and to ensure accountability
- Alignment with company objectives

The PCMS assists the modernization strategy , encouraging digital transformation, public trust, and ensuring effective utilisation of resources.

Business Alignment: PCMS supports the Fiji Police Force Digital Transformation Strategy (2023) by promoting digital modernization, enhancing public trust through transparency, and optimizing resource utilization for improved service delivery.

1.5 References

- Fiji Police Force. (2023). Digital Transformation Strategy 2023-2025.

- IEEE Computer Society. (1998). IEEE Std 830-1998: IEEE Recommended Practice for Software Requirements Specifications..

- W3C – Web Content Accessibility Guidelines (WCAG) 2.1, 2018.

- Java Documentation – Java Platform Standard Edition 17 API Specification.

- Abdulkhaleq, A., Wagner, S., & Leveson, N. (2016). A comprehensive safety engineering approach for software-intensive systems based on STPA. arXiv. https://arxiv.org/abs/1612.03109 arXiv

- Bagies, T., et al. (2024). Classifying software security requirements into the CIA. PMC. PMC

- DAU (Defense Acquisition University). (n.d.). System performance specification. In Acquipedia. dau.edu

- Franch, X. (2023). The state-of-practice in requirements specification. Requirements Engineering Journal. SpringerLink

- IBM. (2025). Performance requirements documentation. IBM

- IEC. (2010). IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems (2nd ed.). International Electrotechnical Commission. Wikipedia

- IEC. (2006). IEC 62304: Medical device software — Software life cycle processes. International Electrotechnical Commission. Wikipedia

- Kadebu, P., et al. (2023). A classification approach for software requirements that considers maintainability as a security requirement. ScienceDirect. ScienceDirect

- Mund, J., Femmer, H., Méndez Fernández, D., & Eckhardt, J. (2017). Does quality of requirements specifications matter? Combined results of two empirical studies. arXiv. arXiv

- Muhamad, F. N. J., Ab Hamid, S. H., Subramaniam, H., Abdul Rashid, R., & Fahmi, F. (2023). Fault-Prone Software Requirements Specification Detection Using Ensemble Learning for Edge/Cloud Applications. Applied Sciences, 13(14), 8368. https://doi.org/10.3390/app13148368 MDPI

- Rączkowska-Gzowska, K., & Walkowiak, A. (2021). What should a good software requirements specification include? Results of a survey. ResearchGate. ResearchGate

2.0 Overall Description

2.1 Product Perspective

The PCMS is a new, self-contained web-based application designed to replace existing manual, paper-based complaint systems. This represents complete digital transformation rather than system evolution.

System Context: PCMS operates as standalone system with planned integration capabilities for:

- National ID verification services
- Email notification systems
- Law enforcement databases
- SMS gateway services

2.2 Product Functions

Major functions of PCMS:

2.2.1 Complaint Submission
Submissions of complaints from citizens
Attachment of evidence/supporting documents
Automated complaint ID generation and tracking

2.2.2 Tracking
Status updates and progress monitoring
Automated complaint ID generation and tracking

2.2.3 Role-Based Dashboards
Officers: view/manage complaints assigned to them
Automated complaint ID generation and tracking
Admins: manage users, assign complaints to officers, oversee complaints

2.2.4 Reporting/Analytics
Generate reports that are based on information provided in each complaint

2.2.5 Security/Access Control
RBAC

2.2.6 Auditing
All actions are to be logged for accountability and traceability purposes

2.3 User Classes and Characteristics

User Class	Description	Expertise Level (Technical)	Accessibility
Citizen	Registered users entitled to complaint submissions	Basic	- Submit - Track
Guest	Unregistered individual submitting complaints	Basic	- Submit only
Officer	Handle complaints	Intermediate	- View complaints - Update status of complaints - Resolve complaints
Admin	Manage users and system	Advanced	- Full access

2.4 Operating Environment

PCMS operates as a browser-accessible platform deployed on secure infrastructure that can be accessed via a browser and hosted via secure infrastructure.

2.4.1 Client Side

Compatible browsers include current versions of Chrome, Firefox (v88+), Safari, and Edge (v90+)

Devices: Desktop, laptop, mobile,tablet

OS:Windows, Mac, IOS, Android

2.4.2 Server Side

OS: Linux Ubuntu/ Windows Server 2019

Web Server: Apache or Nginx

Backend: Java (JDK 17+)

Frontend: HTML, CSS, JavaScript
Database: MySQL 8.0+
Runtime: Java Development Kit(JDK) 17”

2.4.3 Other Software Components:
National ID Verification (citizen authentication)
Analytics tools for decision making

2.4.4 Network Requirements
Minimum 1 Mbps Internet Connection
HTTPS/TLS 1.3 encryption support

2.5 Design and Implementation Constraints

2.5.1 Policy Compliance

Ensure that it aligns with Fiji Police Force’s Digital Transformation Strategy (2023)

2.5.2 Accessibility

W3C’s WCAG 2.1 standards

2.5.3 Technology Stack

Java SE 17 (IT guidelines)

2.5.4 Data Integration

Stable connectivity with law enforcement databases

2.5.5 Security Protocols

HTTPS encryption, login security, RBAC

2.5.6 Hosting Requirements

Government approved infrastructure

2.5.7 Performance Constraints

Support for 10000+ concurrent users
99.5% system uptime requirement

Maximum 3-second page load time

These are to ensure that the PCMS meets the security, usability and modernization goals defined in the product scope.

2.6 User Documentation

Documentation Deliverables
In support of users, the following documents will be provided:

User Manual : Comprehensive guide for guests and citizen
Quick Start Guide: Essential Functions and common tasks
Administrator Guide: System management and configuration instructions
Officer Manual: Case management and investigation procedures
FAQ Document: Frequently asked questions and troubleshooting

2.7 Assumptions and Dependencies

Assumptions

User Readiness - all users will have to have access to the internet and must have basic computer literacy.
Government infrastructure provides reliable hosting and security
Law enforcement personnel will receive adequate system training
National ID verification services

Dependencies

External Services - National ID verification API, email/SMS gateways
Training - All officers and admins must have training on how to use system
Infrastructure - system will be secure and within a government-approved cloud hosting infrastructure
Enhancing - ensure the system can adapt to future changes or enhancements.

Risk Mitigation

Manual verification processes as backup for the automated system

3.0 External Interface Requirements

3.1 User Interfaces

The Police Complaint Management System provides a clean, user-friendly website interface that works well on desktops, tablets, and mobile devices. The design focuses on simplicity, accessibility, and ease of use for all types of users. It has support for responsive design, screen sizes from 320px to 190px width, consistent visual design system with standardized color scheme, and intuitive navigation with breadcrumbs trails and clean action buttons.

3.1.1 Main Users:

- Citizens - can register, log in, file complaints and track progress.
- Tourists/Guests - can fill a quick complaint without registering.
- Police Officers - manage assigned complaints and add updates.
- Administrators - oversee all activity, assign cases, and view reports.

3.1.2 Design Highlights:

- Consistent layout and style across all pages (using CSS and icons)
- Responsive design that adjusts to any screen size.
- Clear navigation with buttons like Login, Register, Back, Submit, etc.
- Forms with dropdown, input fields, and file upload options.
- Color-coded complaint status labels(eg. Pending, Investigating, Resolved)
- Admin Dashboard includes easy-to-read charts using Chart.js.

Each user sees a customized dashboard and pages based on their role.

3.2 Hardware Interfaces

The Police Complaint Management System runs in a web browser, and does not depend heavily on specialized hardware; however it must support interaction with the following hardware interfaces:

3.2.1 User Devices:

- The system can be accessed from desktops, laptops, tablets, and smartphones running on Windows, macOS, Android, or iOS.

- It works best on up-to-date browsers such as Google Chrome, Mozilla Firefox or Microsoft Edge.
- Processing: Minimum dual-core processor at 1.5GHz
- Memory: Minimum 2GB RAM for optimal performance
- Storage: 100MB for available space (for cache and temporary files)
- Display: Minimum 1024x768 resolution

3.2.2 Input Methods:

- Keyboard and mouse (for desktop/laptop interactions)
- Touchscreen (for tablets and smartphones)

3.2.3 File Input Hardware:

- Internal/External Storage: For uploading documents, images, or videos as evidence.
- Mobile device cameras: For capturing and uploading live images
- Scanners: For scanning and uploading evidence

3.2.4 Other Devices (Mainly for Admins/Officers)

- Printers: For generating hard copies of complaints, reports, and dashboards.

3.2.5 Internet Connectivity

- A stable connection via Wi-Fi, LAN, or mobile data is required for accessing the system.
- The application requires secure communication over HTTPS, ensuring encrypted data transmission between client devices and the server.

3.3 Software Interfaces

The POlice Complaint Management System interacts with several software components and libraries:

3.3.1 Operating System(OS) Compatibility:

- Client-side: Any OS with a modern browser.
- Server-side: Linux or Windows depending on deployment

3.3.2 Database:

- System: MYSQL 8.0+ with InnoDB storage engine
- Connection: JDBC driver for java database connectivity
- Data Exchange: SQL queries, stored processes

3.3.3 External Libraries and API's:

- FontAwesome: For UI icons
- Chart.js: For visual data analytics
- JavaScript: Handles page routing (via main.js) and UI interactivity
- File Upload API: For accepting and validating evidence files
- Bootstrap 5.x for responsive design
- JQuery for DOM Manipulation
- Spring Framework 5.x for dependency injection
- Spring security for authorization and authentication
- JasperReports for PDF report generation

3.3.4 Future Integration Possibility:

- Email API's for notification
- SMS Gateways
- National ID

3.3.5 File Handling:

- Upload protocol: HTTPS/HTTPS
- Supported Formats: PDF,DOC,DOCX,JPG
- Security for file type validation, secure storage
- Progress Tracking: Real time upload progress indicators

3.4 Communications Interfaces

PCMS is a web-based platform and relies on internet communication to function effectively. It uses secure, standard communication protocols to ensure smooth and safe data exchange between users and the system.

3.4.1 Web and Network Communication:

- The system is accessed through any web browser (ie. Chrome, Firefox, Safari,Edge)

- All data between the client and the server is transmitted using HTTPS protocol, which provides end-to-end encryption and helps protect sensitive information such as complaint details, user credentials, and uploaded evidence.
- The backend server(RESTful API) communicates with the client-side interface using HTTP requests (GET, POST, PUT, DELETE), typically formatted as JSONfor consistency and readability.
- Web Communication Protocols: HTTPS for all client-server communication

3.4.2 Email Communication:

- The system supports sending automated email notifications for important actions such as:
  - ➢ Complaint Submission and Update
  - ➢ Account Registration and verification
  - ➢ Status changes or officer responses
- Emails will follow standard SMTP protocols and will use secure actions (e.g. TLS encryption) to protect email content.
- Authentication: SMTP authentication with secure credential storage

3.4.3 File Uploads and Forms:

- Complaint forms and evidence upload features are available through secure electronic forms
- Files are uploaded over HTTPS and stored securely on the server
- Accepted formats include images, PDF’s, Word documents, and videos.

3.4.4 Communication Standards

- Protocol Used:
  - ➢ HTTPS (for secure communication)
  - ➢ SMTP with TLS (for secure email delivery)
  - ➢ RESTful API (for internal system operators and modular integrations)
- Data Format:
  - ➢ JSON for data exchange between client and server
  - ➢ MIME types for file uploads

3.4.5 Security and Encryption

- All sensitive communications are encrypted using SSL/TLS certificates

- The system will comply with best practices for data privacy and protection, ensuring confidentiality and integrity during all transmissions.

3.4.6 Synchronization:

- Real-time updates and form submissions are handled through asynchronous communication (AJAX) to ensure the interface remains responsive without needing full page reloads.
- Dashboards for users, officers, and admins reflect live complaint statuses, which are updated automatically as changes occur in the database

4.0 SYSTEM FEATURES

4.1 User Registration and Login

4.1.1 Description and Priority

This feature allows the users(citizens), police officers and the administrator to create an account and login to the system, users access will be restricted only to the relevant feature based on their role. The user role is citizen, Police officer and administrator.

Priority: High

4.1.2 Stimulus/Response Sequence

- Registration stimulus: A user (citizen, police officers and administrator) visits the system registration page and submits the required details to create an account.
- Registration response: The system will then check the inputs by the user and create a new account and sends confirmation email
- Login stimulus: A registered user enters their credentials.
- Login Response: The system will verify the credentials entered by the user and grants access to the appropriate dashboard.
- Login

4.1.3 Functional Requirements

REQ-4.1-01: PCMS will deliver registration forms for citizens requiring full name, email address, phone number, national ID number, and password meeting complexity requirements (minimum 8 characters, mixed case, numbers, special characters). Priority: High

REQ-4.1-02: The system then validates the username and the email during the registration process for a particular user.

REQ-4.1-03: The system should encrypt and safely store all user's passwords.

REQ-4.1-04: The system should allow the registered user to log in to the system with valid username and password

REQ-4.1-05: The system should restrict the access based on the user role such as citizen, police officer and administrator.

REQ-4.1-06: The system should display the specific error message for invalid credentials

REQ-4.1-07:The system shall lock user accounts after 5 consecutive failed login attempts within 15 minutes, requiring administrator unlock or 24-hours automatic unlock
Priority: High

4.2 Complaint Submission and Tracking

4.2.1 Description and Priority

This system feature enables the citizen to file and submit a complaint digitally and track them in real time.

Priority: High

4.2.2 Stimulus/Response Sequence

- Stimulus: The citizen will fill out a complaint form for their complaint and submit it..

- Response: The system will then store the complaint submitted by the user and display a confirmation message.

- Stimulus: The user(citizen) requests the complaint status.

- Response: The system will retrieve the current status of the complaint and display it to the user

4.2.3 Functional Requirement

REQ-4.2-01: PCMS will deliver complaint submission forms requiring complaint title (max 100 characters), type selection from predefined categories, detailed description (max 2000 characters), incident date/time, and location address. Priority: High

REQ-4.2-02: The system shall automatically generate unique alphanumeric complaint IDs using format "FPF-YYYY-NNNNNN" where YYYY is the current year and NNNNNN is a sequential number. Priority: High"

REQ-4.2-03: The system shall support evidence file uploads with maximum 3 files per complaint, each file maximum 10MB, supporting formats: PDF, DOC, DOCX, JPG, PNG, MP4. Priority: High"

REQ-4.2-04: PCMS will deliver a complaint tracking interface showing current status (Submitted, Under Review, Investigating, Resolved, Closed) with timestamp and officer comments. Priority: High"

REQ-4.2-05: The system shall validate complaint submissions requiring all mandatory fields and display specific error messages for incomplete or invalid data. Priority: Medium"

REQ-4.2-06: The system shall send automated email notifications to users within 5 minutes when complaint status changes. Priority: Medium

REQ-4.2-07: The system shall allow guests to submit complaints without registration but require email address for status updates and provide unique tracking codes. Priority: Medium"

4.3 Officer/Admin Dashboard

4.3.1 Description and Priority

This system feature allows the police officers and administrators to check, follow up and manage complaints, monitoring progress with centralized user interface and to manage user's accounts.

Priority: High

4.3.2 Stimulus/Response Sequence

- Stimulus: The police officers log in to their account and open the dashboard.
- Response: The system displays the list of complaints, their assignments and status with filters and sorting in a particular order.

- Stimulus: The admin updating changes to the user’s account details.

- Response: The system stores the changes by updating the current information to the new information update by the admin.

4.3.3 Functional Requirement

REQ-4.3-01: The system displays to the police officers all the user’s complaints on the dashboard.

REQ-4.3-02: The system allows the arranging of complaints by types, status and date that it was submitted.

REQ-4.3-03: The system shall allow the admin to view, update and deactivate a user’s accounts.

REQ-4.3-04: The system should allow the police officers to update the complaint’s progress which will later the user might request.

4.4 Complaint Assignment

4.4.1 Description and Priority

This system feature ensures that the administrator assigns complaints to the appropriate police officer for investigation.

Priority: Medium

4.4.2 Stimulus and Priority

- Stimulus: The administrator assigns a case(complaint) to a police officer.

- Response: The system then notifies the officer that the case is being assigned to them and the complaint is marked assigned in the admin dashboard.

- Stimulus: The admin categorizes the complaints which are urgent and which are not.

- Response: The system will then display it in the officer’s dashboard and then the officer will investigate the case based on its urgency.

4.4.3 Functional Requirement

REQ-4.4-01: The system allows the admin to assign the complaint to the appropriate officer based on the complaint type.

REQ-4.4-02: The system notifies the police officer on which complaint they are assigned to investigate.

REQ-4.4-03: The system shows the categories of the assignment to first work on base on their urgency.

4.5 Security and Data Protection

4.5.1 Description and Priority

This system feature ensures that the data stored in the system such as user credential and complaints information is safe from unauthorized access.

Priority: High

4.5.2 Stimulus/Response Sequence

- Stimulus: Unauthorized users attempt to access the system sensitive data.

- Response: The system firewall blocks the unauthorized user from accessing the system data.

4.5.3 Functional Requirement

REQ-4.5-01: System using https to ensure the safety of data transfer.

REQ-4.5-02: The system encrypts all the user details such as the user password.

REQ-4.5-03: System shall restrict the user access based on the user role.

REQ-4.5-04: The system shall install a firewall to block external access.

REQ-4.5-05: Monitor the suspicious activity and alert the administrator when there is a security breach.

4.6 Notifications

4.6.1 Description and Priority.

This system updates the citizen about their complaint status and notify the officer about a new assignment or assignment changes.

Priority: Medium

4.6.2 Stimulus/Response Sequence

- Stimulus: A complaint status changes from investigation to resolve.
- Response: The system will send a notification to the citizen about the update.
- Stimulus: A new complaint is assigned to an officer.
- Response: The officer will be notified by the system.

4.6.3 Functional Requirement

REQ-4.6-01: The system notified the citizen of a complaint status change.

REQ-4.6-02: The system notified the officer of a new complaint.

REQ-4.6-03: The system may notify the admin of a security breach.

5.0 Other Non-functional Requirements

5.1 Performance Requirements

Performance requirements are defined by how efficiently the system operates under various workloads, focusing on aspects such as speed, response time, resource utilization, and scalability. A system requirement might say, for instance, " 99% of transactions must complete within 2 seconds under peak load. " Design strategies, capacity planning, and architectural decisions are all influenced by these requirements (IBM, 2025). Performance specifications authorize the vendor's flexibility in the defense and acquisition domains by outlining expected results without dictating implementation (MIL-STD-961E, per DAU documentation).

REQ-5.1-01: The system shall respond to user requests within 3 seconds for 95% of transactions under normal load conditions (up to 100 concurrent users). Priority: High

REQ-5.1-02: The system shall support up to 1000 concurrent users during peak usage periods with response times not exceeding 5 seconds. Priority: Medium

REQ-5.1-03: The system shall process complaint submissions and generate confirmation within 10 seconds including file uploads up to 30MB total size. Priority: High

REQ-5.1-04: The system shall achieve 99.5% uptime availability excluding planned maintenance windows (maximum 4 hours monthly). Priority: High

REQ-5.1-05: The system shall handle database queries returning complaint lists within 2 seconds for result sets up to 1000 records. Priority: Medium

REQ-5.1-06: The system shall support file upload progress tracking with real-time status updates for files larger than 5MB. Priority: Low

5.2 Safety Requirements

The safety requirements are to reduce or eliminate risks that could cause harm to people, property, or the environment. Some safety standards, such as IEC 62304 (for medical device software), must be followed when developing safety-critical software. To guarantee a predictable, safe failure mode and measure risk, these standards call for a safety lifecycle, formal specification methods, modular and testable design, code review, and multi-layer testing (IEC, 2010; IEC, 2006). Furthermore, STPA (System-Theoretic Process Analysis) ensures that safety constraints are incorporated into the architecture and verification processes by integrating hazard analysis and safety requirements derivation within the software engineering lifecycle(Abdulkhaleq et al., 2016).

REQ-5.2-01: The system shall implement automatic data backup procedures every 24 hours with backup verification and off-site storage. Priority: High

REQ-5.2-02: The system shall implement input validation and sanitization preventing data corruption from malformed inputs or injection attacks. Priority: High

REQ-5.2-03: The system shall maintain audit trails for all data modifications enabling recovery and investigation of system issues or security incidents. Priority: Medium

REQ-5.2-04: PCMS will deliver disaster recovery procedures with maximum 24-hour recovery time objective (RTO) and 4-hour recovery point objective (RPO). Priority: High

5.3 Security Requirements

Security requirements, which are frequently articulated through the CIA triad, specify safeguards for auditability, authorization, confidentiality, integrity, and authentication. To facilitate early detection and enforcement of security controls, Bagies et al. (2024) propose a machine learning-based approach for categorizing requirements during the requirements engineering phase. Furthermore, Kadebu et al. (2023) contend that since unauthorized changes may result in vulnerabilities, maintainability should be considered a security concern as well.

REQ-5.3-01: The system shall implement multi-factor authentication for administrator accounts requiring password plus email or SMS verification. Priority: High

REQ-5.3-02: The system shall enforce password complexity requirements including minimum 8 characters, mixed case, numbers, and special characters with 90-day expiration for officers and administrators. Priority: High

REQ-5.3-03: The system shall implement session timeout after 30 minutes of inactivity for officer and administrator accounts, 60 minutes for citizen accounts. Priority: Medium

REQ-5.3-04: The system shall log all security-related events including failed login attempts, privilege escalations, and administrative actions with non-repudiation capabilities. Priority: High

REQ-5.3-05: The system shall encrypt all sensitive data at rest using AES-256 encryption including personal information, complaint details, and authentication credentials. Priority: High

REQ-5.3-06: The system shall implement secure password recovery through email verification with temporary reset tokens expiring within 24 hours. Priority: Medium

5.4 Software Quality Attributes

Reliability, usability, maintainability, portability, and testability are important architectural qualities that, when feasible, should be quantified. Strong process assurance supports quality for safety-critical software by influencing internal attributes like code structure, which in turn affects external reliability and functionality (IEC 61508 guidance). Process standards such as ISO 25010 offer comprehensive quality models. Furthermore, downstream phases are greatly impacted by variations in the quality of requirements specifications: Mund et al. (2017) demonstrate how SRS quality flaws can impede efficient communication and raise development risk, particularly in safety-critical domains.

REQ-5.4-01: The system shall handle unexpected errors gracefully without exposing sensitive system information to users. Priority: High

REQ-5.4-02: The system shall implement automated error reporting and logging for system failures and performance degradation. Priority: Medium

Usability: The system shall enable new users to complete basic tasks (registration, complaint submission) within 10 minutes without training, with user satisfaction scores above 4.0/5.0.

REQ-5.4-03: PCMS will deliver consistent navigation and interface elements across all user roles and device types. Priority: High

REQ-5.4-04: The system shall support accessibility features including screen reader compatibility and keyboard navigation. Priority: Medium

Maintainability: The system shall support hot-fixes and minor updates with maximum 15 minutes downtime and major updates with maximum 4 hours scheduled maintenance.

REQ-5.4-05: The system shall maintain comprehensive system documentation updated with each release cycle. Priority: Low

Portability: The system shall operate consistently across supported browsers and operating systems without requiring client-side plugins or extensions.

REQ-5.4-06: The system shall maintain identical functionality across Chrome, Firefox, Safari, and Edge browsers with versions released within the past 2 years. Priority: High

5.5 Business Rules

Business rules articulate the operational limitations that control how users behave and how the system works. They imply functional enforcement even though they are not functional requirements in and of themselves, for example, "only managers can approve purchase orders," since these rules govern roles, permissions, and business logic modules. Franch (2023) stresses the significance of precisely capturing them in SRS documents.

BR-01: Only verified citizens with valid Fiji national ID numbers may register for full system access including complaint tracking and history viewing.

BR-02: Guest users may submit complaints but cannot access complaint history or receive direct notifications beyond initial confirmation email.

BR-03: Officers may only view and modify complaints assigned to them or unassigned complaints within their designated jurisdiction or specialization area.

BR-04: Administrators may reassign complaints only when providing written justification and recording the reason in system audit logs.

BR-05: Complaint data must be retained for minimum 7 years per Fiji legal requirements with secure archival procedures after active investigation closure.

BR-06: Personal information of complaint submitters shall be accessible only to assigned investigating officers and authorized administrators on a need-to-know basis.

BR-07: System administrators must have security clearance and undergo annual background verification before accessing sensitive law enforcement data.

BR-08: All complaint status changes must include mandatory progress comments from the responsible officer before the system will accept the update.

BR-09: High-priority complaints must be acknowledged by assigned officers within 4 hours during business days, 8 hours during weekends.

BR-10: Citizens may submit a maximum 5 complaints per calendar month to prevent system abuse while allowing legitimate multiple incident reporting.

6.0 Other Requirements

6.1 Database Requirements

REQ-6.1-01: The system shall implement normalized relational database design with referential integrity constraints preventing orphaned records and maintaining data consistency. Priority: High

REQ-6.1-02: The system shall support automated database backup procedures with point-in-time recovery capabilities for data restoration within any 15-minute window. Priority: High

REQ-6.1-03: The system shall implement database indexing strategies ensuring query response times under 2 seconds for datasets up to 100,000 complaints. Priority: Medium

REQ-6.1-04: The system shall maintain database connection pooling with automatic connection recycling preventing memory leaks and connection exhaustion. Priority: Medium

6.2 Internationalization Requirements

REQ-6.2-01: The system shall support English as the primary language with unicode UTF-8 character encoding enabling future localization. Priority: Medium

REQ-6.2-02: The system shall implement resource bundle architecture preparing for future translation to Fijian and Hindi languages. Priority: Low

REQ-6.2-03: The system shall handle right-to-left text display and locale-specific date/time formatting for future international deployment. Priority: Low

6.3 Legal and Compliance Requirements

REQ-6.3-01: The system shall comply with Fiji Privacy Act 2003 requirements for personal information collection, storage, and access controls. Priority: High

REQ-6.3-02: The system shall implement data retention policies meeting law enforcement requirements with automatic archival after case closure. Priority: High

REQ-6.3-03: PCMS will deliver audit trail capabilities supporting legal discovery processes and court proceedings. Priority: High

REQ-6.3-04: The system shall implement data anonymization procedures for statistical reporting while maintaining individual privacy protection. Priority: Medium

6.4 Integration Requirements

REQ-6.4-01: PCMS will deliver RESTful API endpoints for future integration with national databases, court systems, and inter-agency information sharing platforms. Priority: Medium

REQ-6.4-02: The system shall implement webhook capabilities for real-time data synchronization with external law enforcement systems. Priority: Low

REQ-6.4-03: The system shall support standard data export formats (CSV, XML, JSON) for integration with reporting and analytics tools. Priority: Medium

REQ-6.4-04: The system shall implement secure API authentication using industry-standard protocols (OAuth 2.0, JWT tokens) for external system integration. Priority: Medium

6.5 Audit and Monitoring Requirements

REQ-6.5-01: The system shall maintain comprehensive audit logs for all user activities including login attempts, data access, complaint submissions, and system changes for a minimum 3 years. Priority: High

REQ-6.5-02: The system shall implement real-time monitoring dashboards showing system performance metrics, user activity patterns, and security events. Priority: Medium

REQ-6.5-03: The system shall generate automated compliance reports for management review including user access patterns, data retention status, and security incident summaries. Priority: Medium

REQ-6.5-04: The system shall implement tamper-evident log storage preventing unauthorized modification or deletion of audit records. Priority: High

Appendix A: Glossary

Administrator: System user with full access privileges for user management, system configuration, and complaint oversight. Requires security clearance and administrative training.

API (Application Programming Interface): Set of protocols and tools allowing different software applications to communicate and share data with the PCMS.

Citizen: Registered system user who is a resident or citizen of Fiji with verified national identification able to submit complaints and track their progress.

Complaint: Formal submission detailing alleged misconduct, criminal activity, or service issues requiring law enforcement attention and investigation.

Guest: Unregistered system user with limited access for complaint submission only, without account creation or historical access capabilities.

HTTPS (Hypertext Transfer Protocol Secure): Encrypted communication protocol ensuring secure data transmission between client browsers and the PCMS server.

JWT (JSON Web Token): Secure method for transmitting information between parties as digitally signed tokens used for API authentication.

MTBF (Mean Time Between Failures): Average time interval between system failures, measured in hours of continuous operation.

MTTR (Mean Time To Recovery): Average time required to restore system functionality after a failure or outage occurs.

Officer: Law enforcement personnel authorized to investigate and manage complaints within their jurisdiction, with specialized system access for case management.

RBAC (Role-Based Access Control): Security method restricting system access based on user roles and permissions, preventing unauthorized data access.

RPO (Recovery Point Objective): Maximum acceptable amount of data loss measured in time during disaster recovery scenarios.

RTO (Recovery Time Objective): Maximum acceptable amount of time to restore system functionality during disaster recovery procedures.

SRS (Software Requirements Specification): Comprehensive document describing functional and non-functional system requirements for development and testing purposes.

TLS (Transport Layer Security): Cryptographic protocol providing secure communication over computer networks, successor to SSL.

UUID (Universally Unique Identifier): 128-bit number used to uniquely identify information in computer systems without central coordination.

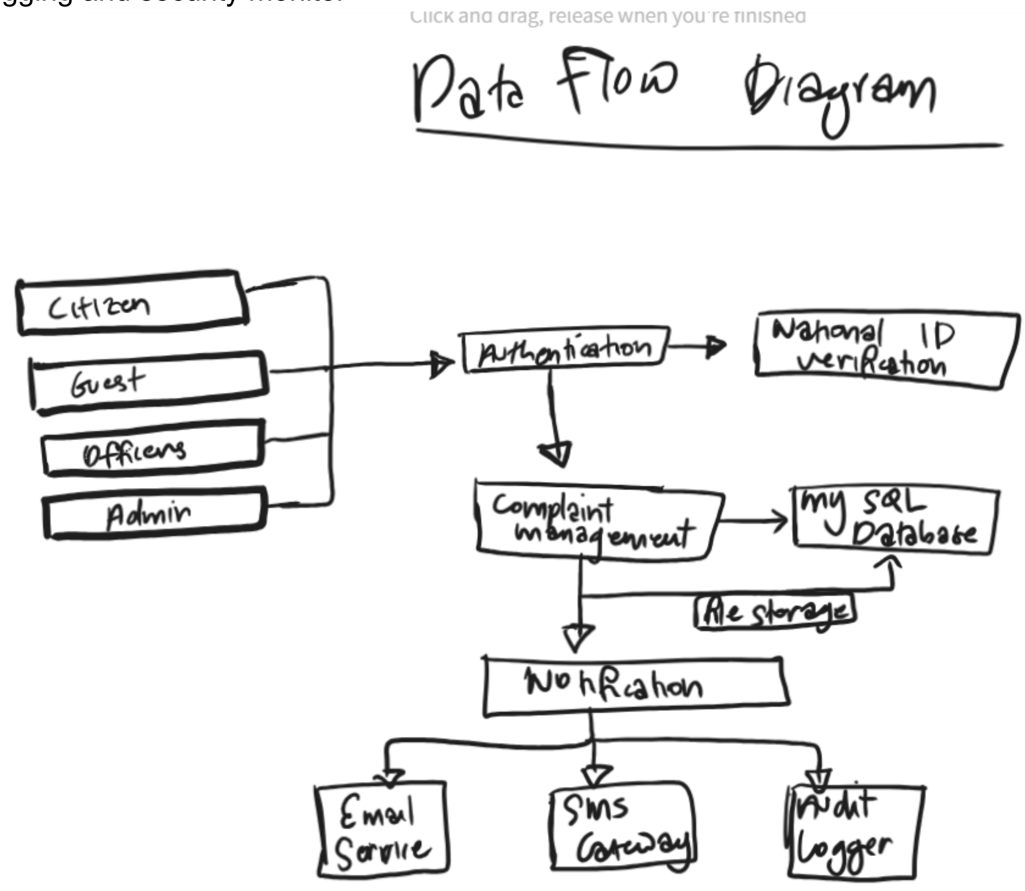
Appendix B: Analysis Models

B.1 Data Flow Diagram

High-Level System Data Flow: Visual representation showing information movement between users (Citizens, Officers, Administrators), core system components (Authentication, Complaint Management, Database), and external services (Email, SMS, National ID Verification).

Key Data Flows:

- User registration and authentication data flows
- Complaint submission and evidence upload processes
- Status update and notification distribution
- Administrative management and reporting data paths
- Audit logging and security monitoring flows

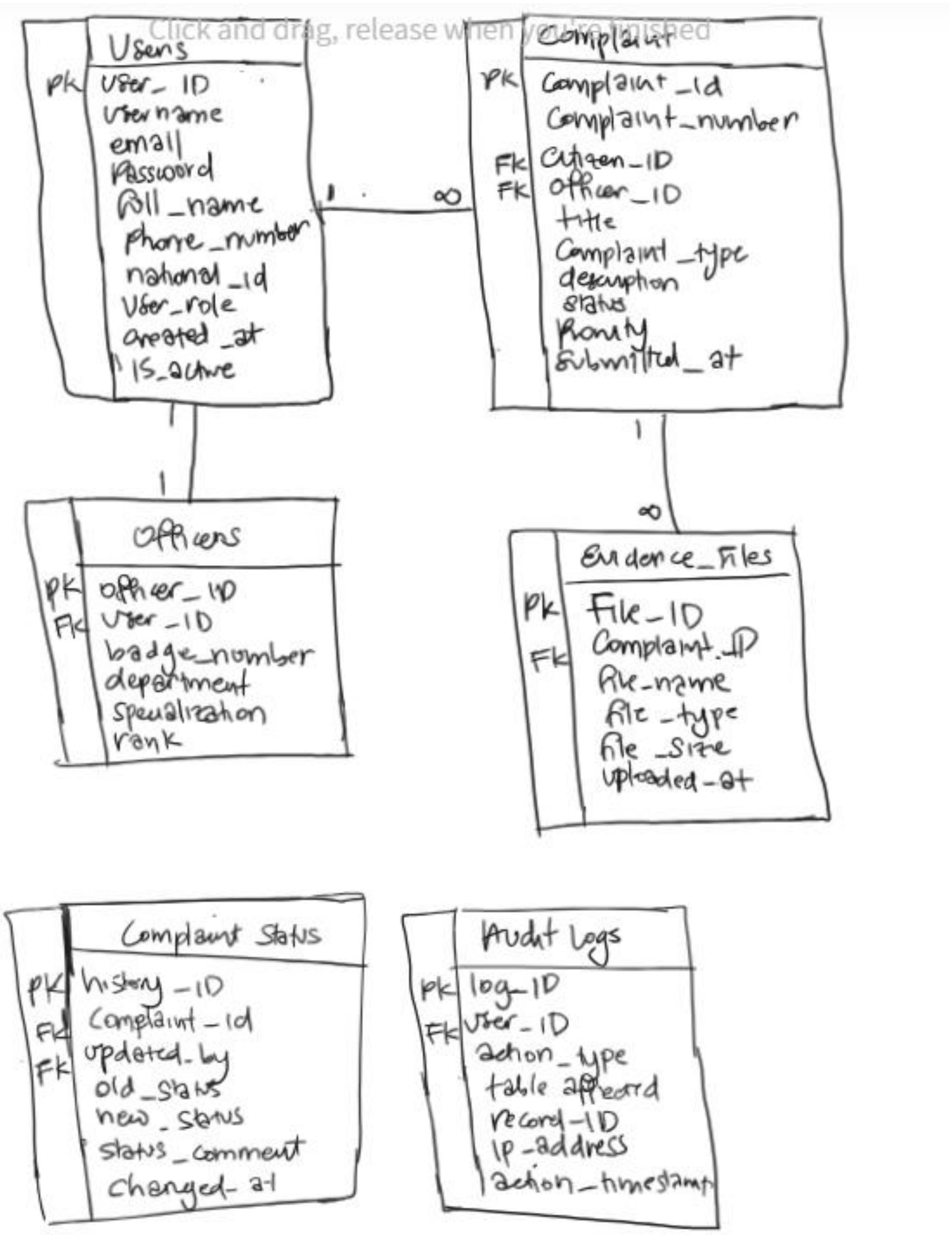


B.2 Entity Relationship Diagram

Database Schema Representation: Complete ERD showing relationships between primary entities including Users, Complaints, Officers, Assignments, Evidence Files, Audit Logs, and System Configuration tables.

Primary Entities:

- Users (Citizens, Officers, Administrators)
- Complaints (with status, priority, and assignment tracking)
- Evidence (file attachments linked to complaints)
- Audit Logs (comprehensive activity tracking)
- System Configuration (roles, permissions, settings)

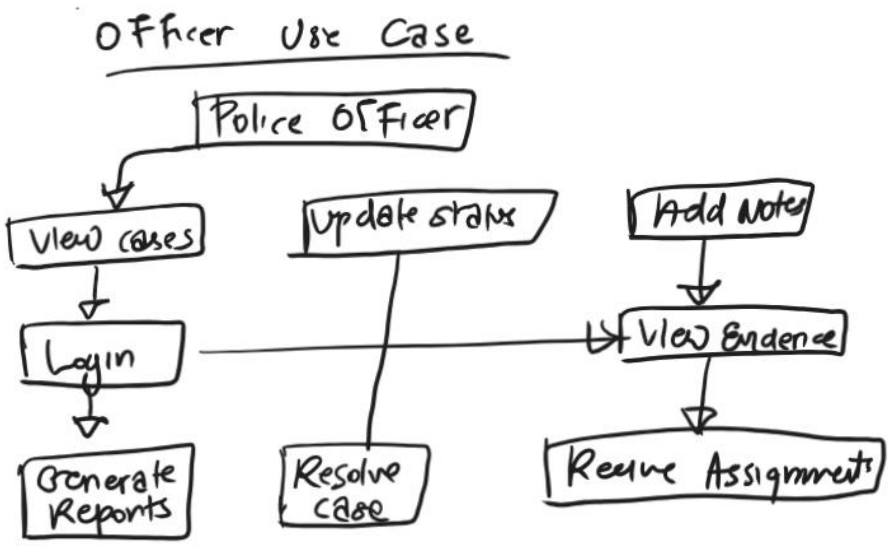

Click and drag, release when you're finished
Users
PK
User_ ID
Username
email
Password
full_name
phone_number
national_id
User_role
created_at
is_active
1
∞
Complaint
PK
Complaint_id
Complaint_number
FK
Citizen_ID
FK
officer_ID
title
Complaint_type
description
status
Priority
Submitted_at
1
1
1
∞
Officers
PK
officer_ID
FK
User_ID
badge_number
department
Specialization
rank
Evidence_Files
PK
File_ID
FK
Complaint_ID
File_name
file_type
file_size
uploaded_at
Complaint Status
PK
history_ID
FK
Complaint_id
FK
updated_by
old_status
new_status
status_comment
changed_at
Audit Logs
PK
log_ID
FK
User_ID
action_type
table affected
record_ID
ip_address
action_timestamp

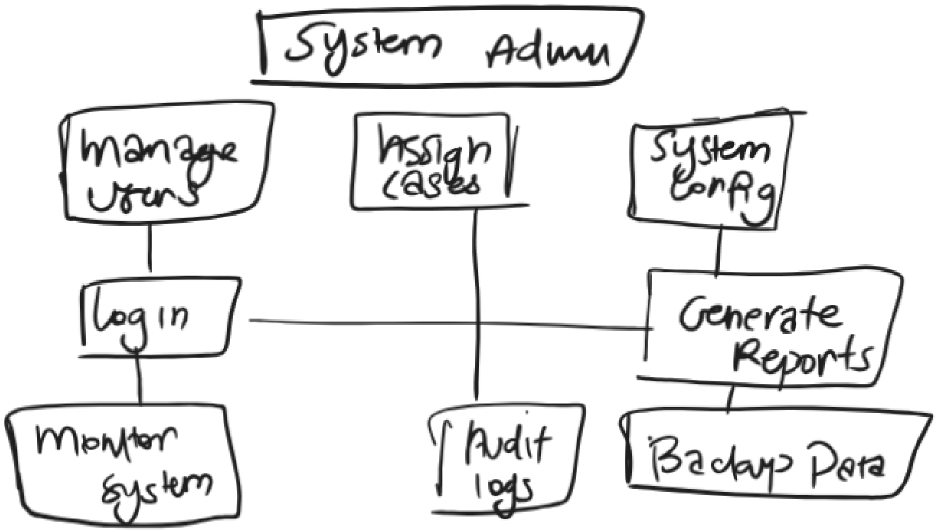
B.3 Use Case Diagrams

System Functionality Overview: Visual representation of system functionality and user interactions for each user class showing primary and secondary use cases.

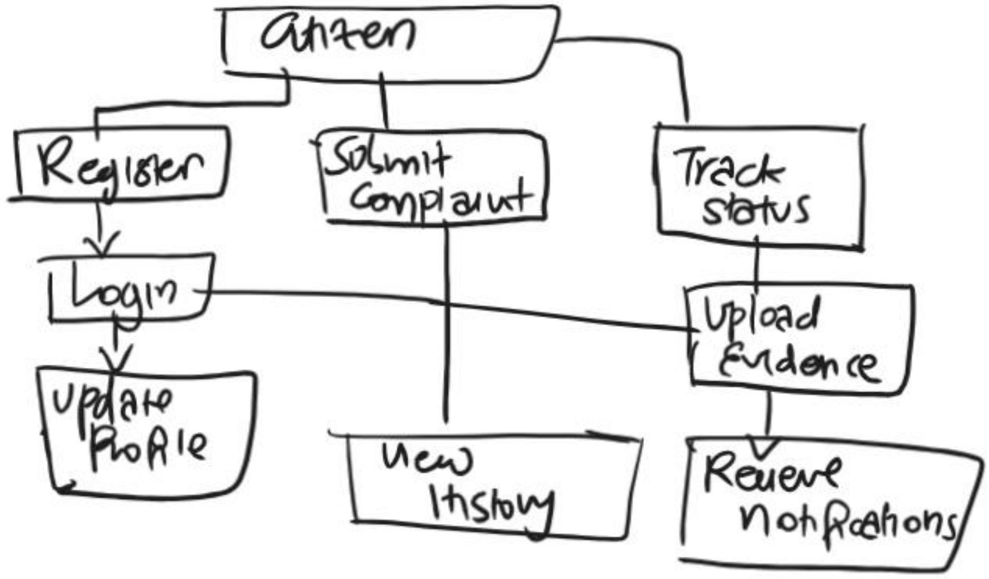
Primary Use Cases:

- Citizen: Register, Login, Submit Complaint, Track Status, Upload Evidence
- Officer: Manage Assigned Complaints, Update Status, Add Investigation Notes
- Administrator: User Management, Complaint Assignment, System Configuration, Generate Reports





Citizen use cases

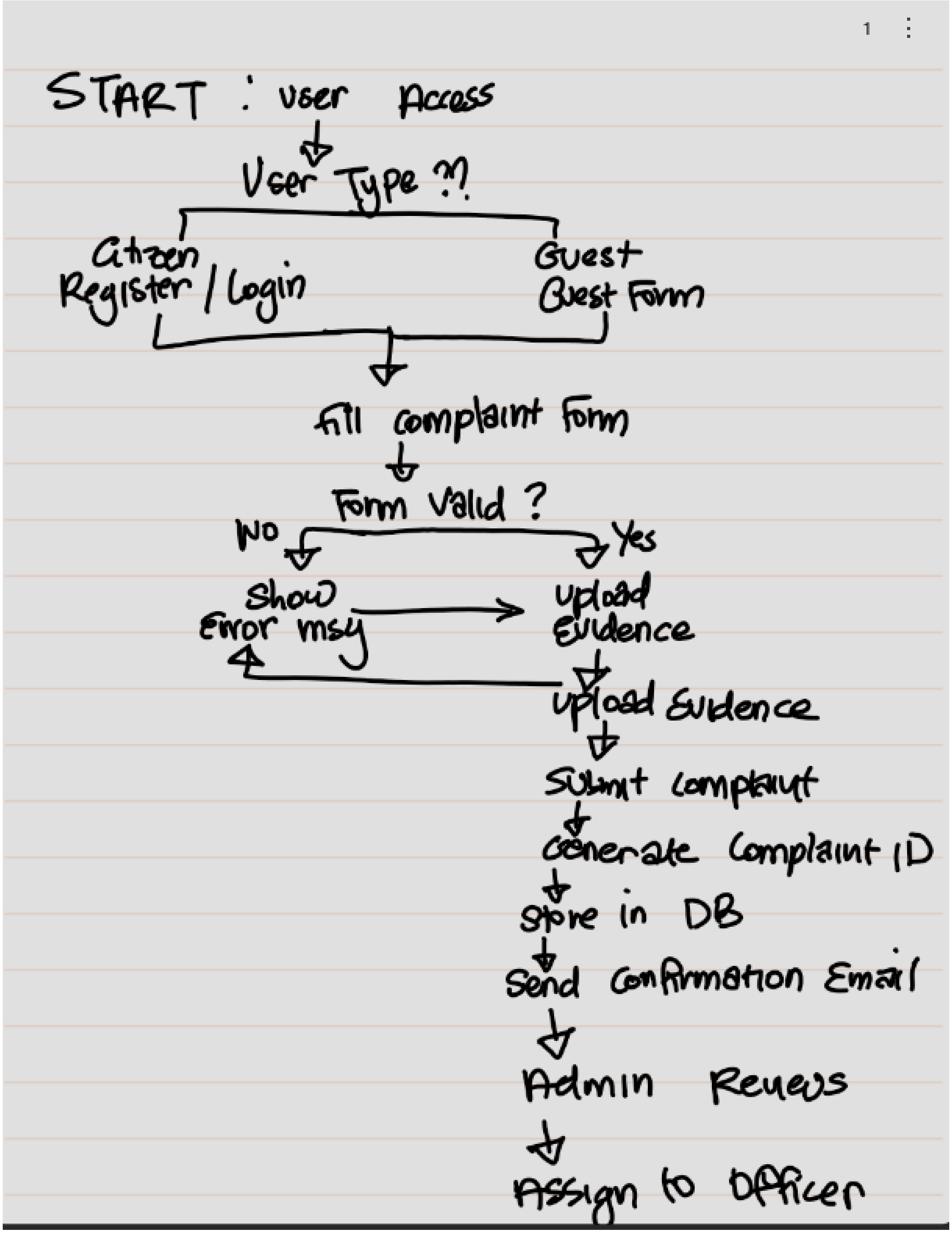


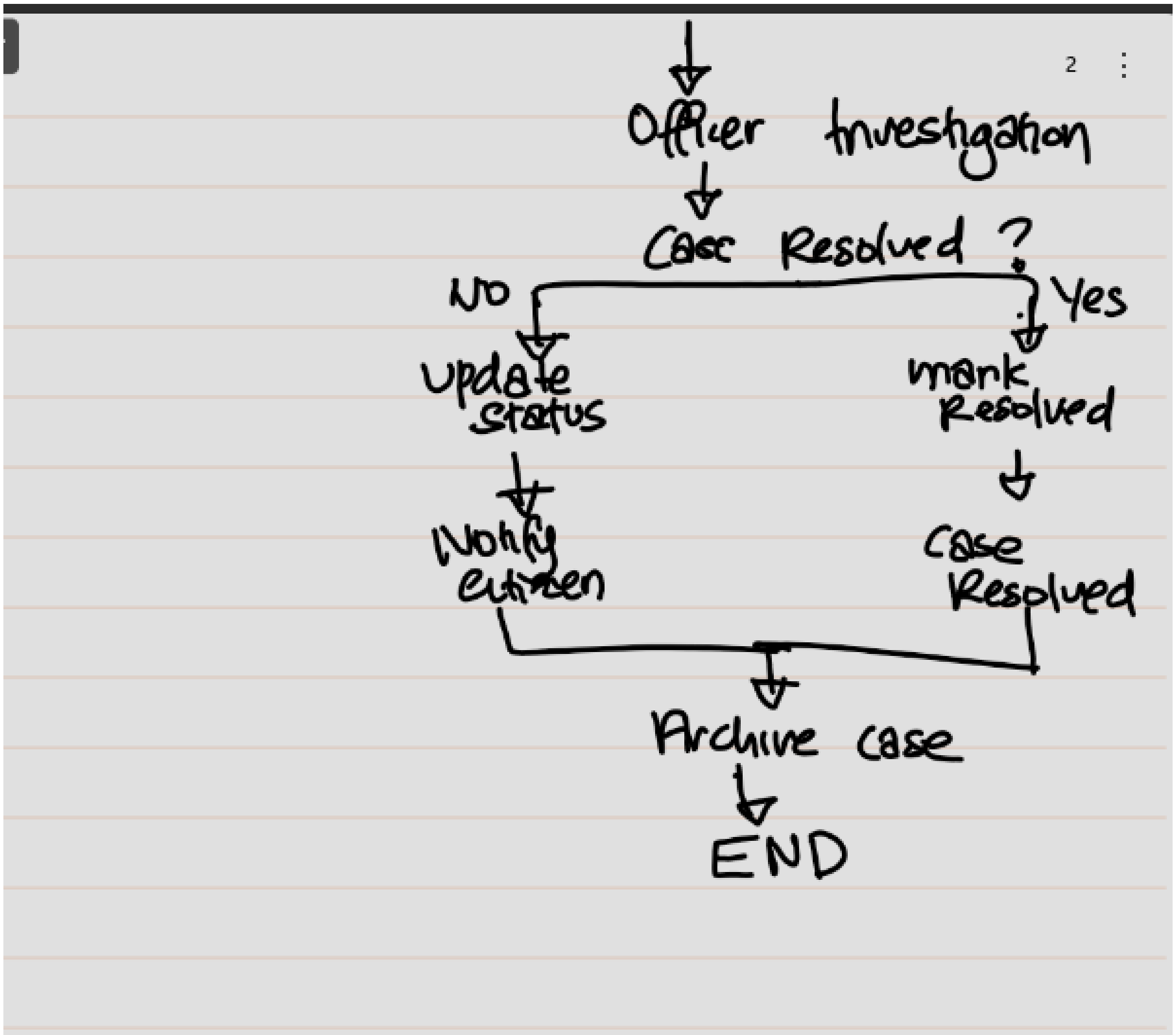
B.4 System Architecture Diagram

Technical Architecture Overview: High-level architecture showing web servers, application servers, database systems, and external service integration points including load balancers, security components, and backup systems.

Architecture Components:

- Presentation Layer (Web Interface, Mobile Responsive Design)
- Application Layer (Business Logic, API Services)
- Data Layer (MySQL Database, File Storage)
- Integration Layer (External Services, API Gateway)
- Security Layer (Authentication, Authorization, Encryption)


START : user Access
User Type ?!
Citizen
Register / Login
Guest
Guest Form
Fill complaint Form
Form Valid ?
No
Yes
Show
Error msg
Upload
Evidence
Upload Evidence
Submit complaint
Generate Complaint ID
Store in DB
Send Confirmation Email
Admin Reviews
Assign to Officer


2
Officer Investigation
Case Resolved ?
No
Yes
Update status
Mark Resolved
Notify citizen
Case Resolved
Archive case
END

Appendix C: To Be Determined List

TBD-01: Specific National ID verification API endpoints and data formats pending government service provider selection and security clearance approval.

TBD-02: SMS gateway service provider and API specifications to be determined based on cost analysis, coverage requirements, and government procurement contracts.

TBD-03: Exact server hardware specifications and hosting infrastructure details pending IT department budget approval, vendor selection, and security compliance review.

TBD-04: Integration specifications with existing law enforcement databases pending security clearance approval, data sharing agreements, and technical compatibility assessment.

TBD-05: Specific backup and disaster recovery procedures pending establishment of secondary data center location and government infrastructure requirements.

TBD-06: User training program content, delivery methods, and certification requirements to be developed following user acceptance testing, stakeholder feedback collection, and training needs assessment.

TBD-07: Go-live deployment strategy and phased rollout timeline pending stakeholder approval, resource allocation, and change management planning.

TBD-08: Mobile application development specifications for iOS and Android platforms to be determined based on user demand analysis and budget allocation.

TBD-09: Advanced analytics and reporting requirements pending management review of initial system capabilities and business intelligence needs assessment.

TBD-10: System integration with court management systems pending legal department approval and technical feasibility study completion.