Futurist IT ***SafeNet*** *SRS V 1.2*

SafeNet: Bridging Communities and Law Enforcement for Enhanced Public Safety

Software Requirements Specification

September 18, 2024

Group: 03

Supervised By: Md. Al-Amin

Name	ID
Md Noman Islam	21-45453-3
Md Nasimul Islam	21-45465-3
Sadia Islam Mim	20-43436-1
Sharmin Jahan	21-45869-3

Table of Contents

Introduction

Project Name: SafeNet

Ministry: Home Affairs

Platform: SafeNet is a platform aimed at fostering trust and collaboration between communities and law enforcement agencies. The system offers quick access to police and medical emergency services, promotes officer accountability, and enhances public safety through community engagement in crime prevention.

Overview: The goal of this SRS is to ensure a clear understanding of the SafeNet platform's functionalities and to guide the development, implementation, and testing processes. By adhering to the requirements outlined in this document, SafeNet aims to provide a reliable and user-friendly solution that enhances public safety, and fosters trust between law enforcement and the community.

Purpose: The purpose of this Software Requirements Specification (SRS) document is to provide a detailed description of the SafeNet platform, a comprehensive solution designed to enhance community safety and improve the effectiveness of law enforcement agencies. This document outlines the functional requirements and features of SafeNet, which aims to build trust between the community and law enforcement, facilitate quick access to emergency services, and promote positive interactions between citizens and officers.

Business Requirement

Vision: The vision for SafeNet is to revolutionize the relationship between law enforcement agencies and the community by creating a trusted, transparent, and efficient platform that enhances public safety. SafeNet envisions a future where citizens have immediate and reliable access to law enforcement support, where police interactions are accountable and constructive, and where community involvement in crime prevention is actively encouraged and facilitated. By bridging gaps between police and the public, SafeNet aims to foster a safer and more cooperative society.

Scope: SafeNet is a multi-functional platform intended to bridge the gap between law enforcement agencies and the community. It provides a range of features to support public safety, streamline emergency responses, and foster transparent and accountable interactions between police officers and citizens. The primary features include police identification verification, nearest police station and health center locators, a police officer rating and review system, and an anonymous crime reporting tool. The platform is designed to operate as a mobile and web application, accessible to users across various devices.

Business Rules / Objectives

1. Enhance Public Safety:

Objective: Provide users with quick and reliable access to police and medical emergency services.

Benefit: By offering features such as location-based services for the nearest police stations and health centers, SafeNet ensures that individuals can swiftly find help in critical situations, thereby improving response times and overall public safety.

2. Build Trust and Transparency:

Objective: Strengthen the trust between the community and law enforcement agencies through transparency and accountability.

Benefit: The Police Identification Verification Feature and the Police Officer Rating and Review System are designed to ensure that police interactions are transparent, with officers' identities confirmed and feedback on their performance collected, leading to increased trust and improved relationships between officers and the community.

3. Promote Positive Behavior Among Officers:

Objective: Encourage law enforcement officers to exhibit positive behavior and professionalism.

Benefit: The ability for citizens to rate and review their interactions with police officers provides feedback that can lead to continuous improvement in officer conduct and service quality, promoting a culture of accountability and positive behavior.

4. Encourage Community Involvement:

Objective: Engage the community in crime prevention efforts by providing a platform for anonymous reporting of crimes and suspicious activities.

Benefit: The Anonymous Crime Reporting Feature allows citizens to report incidents without fear of retaliation, thus increasing community involvement in maintaining public safety and aiding law enforcement in crime detection and prevention.

5. Reduce Response Times:

Objective: Minimize the time it takes for law enforcement and emergency services to respond to incidents.

Benefit: By providing accurate location data and direct communication options through the Nearest Police Station & Health Center Locator Feature, SafeNet helps ensure that emergency services can reach individuals faster, thereby improving the effectiveness of interventions during critical situations.

6. Foster Collaborative Partnerships:

Objective: Develop collaborative relationships between law enforcement agencies and the community.

Benefit: SafeNet's features are designed to support and facilitate collaboration, creating an environment where both law enforcement and community members can work together more effectively in preventing crime and addressing safety concerns.

Constraints

➢ Operational and Technical Constraints

- SafeNet must comply with all relevant laws and regulations regarding public safety, law enforcement procedures, data protection, and privacy in Bangladesh.
- The platform must adhere to the Bangladesh Information and Communication Technology (ICT) Act and any other relevant national data security regulations.
- The platform must operate within the constraints of the current infrastructure in police stations and health centers, which may not support advanced technology uniformly across all regions.
- The system's implementation and maintenance must operate within the allocated budget and resource constraints, ensuring that both hardware and software requirements are met without exceeding the financial plan.
- Availability of reliable internet and communication networks across rural and urban regions of Bangladesh may affect the real-time performance of SafeNet, requiring fallback procedures for low-coverage areas.
- Given the sensitive nature of the information handled, SafeNet must implement robust encryption protocols and access control mechanisms to prevent unauthorized access or data breaches. This may impose constraints on processing time and system architecture.
- The platform must guarantee anonymity for users submitting crime reports, ensuring no data traceability that could compromise the safety of users who report suspicious activities.
- The system must support a large user base, including all citizens of Bangladesh with valid identification cards, as well as law enforcement and emergency health personnel. Any scalability limitations in the system infrastructure must be managed to ensure consistent and reliable performance.
- SafeNet's functionality depends on real-time location services and communication systems (GPS, mobile networks). Constraints may arise from limited accuracy in location tracking, network coverage issues, or disruptions in service, particularly in remote areas.
- The platform must be able to provide seamless real-time communication and accurate location data for emergency services, subject to the limitations of the underlying technology and network conditions.
- Law enforcement personnel and healthcare providers must be trained to use the platform effectively. Constraints in training resources or resistance to technological adoption among users may impact the success of the platform's deployment.\
- SafeNet must function smoothly across multiple platforms (web, mobile) and devices with varying operating systems (iOS, Android, Windows, etc.). Limitations in cross-platform compatibility or performance variations across devices may affect user experience.
- Ongoing system maintenance, bug fixes, and updates must be conducted without disrupting service availability. However, resource limitations for long-term support and updates may constrain the frequency or scope of future enhancements to the platform.

Identify the Stakeholders

1. Customers

- Who have direct connection with the platform

- Police Department
- Hospital Emergency Medical Services
- General Public
- Platform Experts

2. Users

- Which stakeholders directly interact with the platform

- Every Bangladeshi Citizen with Valid ID Card
- Police Officers & Police Personnel
- Emergency Health Provider
- Developers

3. Product Champion

- Who will advocate, promote platform's adoption and continuous improvements.

- Influential Community Member.
- Policy Maker
- High Ranked Police Officer
- Police Personnel
- Operator of Emergency Health Provider

Requirement Elicitation

Questionnaire: A structured questionnaire was distributed to law enforcement agencies, healthcare centers, and local government representatives to identify the key functionalities and features they require. The questionnaire focused on understanding the specific challenges faced in public safety, incident reporting, and law enforcement response.

- **Questionnaire for Law Enforcement Agencies**
  1. What is your role within the law enforcement agency?
  2. How frequently do you handle emergency incidents that require immediate response?
  3. What are the common types of incidents that you deal with?
  4. What are the biggest challenges you face with the current incident reporting system?
  5. How long does it usually take to respond to incidents from the time they are reported?
  6. How do you currently track incident locations, and what difficulties do you encounter in this process?
  7. Are there any gaps in communication between officers during an ongoing incident?
  8. How important is data security and encryption for communication between officers and the public?
  9. Would you prefer a mobile app, desktop system, or both for managing incident reports?
  10. Do you need integration with existing databases (e.g., criminal records, vehicle registration)?
  11. Would you benefit from an alert system that notifies officers of high-priority incidents?

- **Questionnaire for Healthcare Centers**
  1. What is your role in the healthcare center?
  2. How often do you deal with emergency medical incidents?
  3. What is the current process for receiving and managing emergency cases?
  4. What are the primary challenges you face when coordinating with law enforcement during emergencies?
  5. How do delays in communication or response affect your ability to provide timely medical care?
  6. How do you currently manage real-time information for emergency cases?
  7. How important is it to integrate ambulance services and other medical emergency response units into a public safety system?
  8. Would you prefer to use mobile devices, desktop computers, or both to manage emergency communication?
  9. How would a real-time location tracking feature improve emergency medical response times?

- **Questionnaire for Local Government Representatives**
  1. What is your role in the local government?
  2. What public safety responsibilities do you oversee in your position?
  3. How do you currently manage incidents related to public safety and law enforcement?
  4. What are the main challenges you face in ensuring public safety and law enforcement coordination?
  5. How effective is communication between law enforcement, healthcare, and other government agencies during crises?
  6. What difficulties do you encounter in monitoring high-risk areas within your jurisdiction?
  7. How important is it for local government departments to have access to real-time data from law enforcement and healthcare services?

Interviews: In-depth interviews were conducted with various stakeholders, including police officers, emergency responders, and community leaders, to gain insights into their operational workflows, pain points, and the practical aspects of integrating SafeNet into their existing systems. These interviews allowed for a deeper understanding of the nuances and constraints that may not have been captured through questionnaires.

Surveys: Online surveys were conducted for the general public to gather feedback on their concerns, experiences, and expectations regarding public safety and the ease of reporting incidents. This method helped understand the public's perspective on the desired usability and accessibility of the platform.

1. What is your age group?
    a. Under 18
    b. 18-24
    c. 25-34
    d. 35-44
    e. 45-54
    f. 55 and above

2. What is your primary mode of communication with law enforcement (if any)?
    a. Phone calls
    b. In-person visits
    c. I have not communicated with law enforcement

3. How aware are you of the public safety services available in your area?
    a. Very aware
    b. Somewhat aware
    c. Not aware at all

4. How often do you witness or experience public safety incidents (e.g., accidents, theft, emergencies) in your neighborhood?
    a. Frequently
    b. Occasionally
    c. Rarely
    d. Never

5. Have you ever needed to report a public safety incident (e.g., crime, fire, health emergency)?
    a. Yes
    b. No

6. If yes, how did you report the incident?
    a. Called emergency services (e.g., 999)
    b. Filed a report online
    c. Visited a police station
    d. Other (please specify)

7. How satisfied were you with the response time of law enforcement or emergency services?
    a. Very satisfied
    b. Satisfied
    c. Neutral
    d. Dissatisfied
    e. Very dissatisfied

8. What challenges did you face while reporting the incident (if any)?
    a. Slow response time
    b. Difficulty in communicating details
    c. Lack of follow-up
    d. No challenges

9. What features would you find most useful in a public safety platform (SafeNet)?
    a. Real-time incident reporting
    b. Anonymous reporting
    c. GPS-based location sharing
    d. Alerts for emergencies in my area
    e. Direct communication with law enforcement
    f. Emergency contact registration

10. Would you prefer using a mobile app, website, or both for reporting incidents and receiving alerts?
    a. Mobile app
    b. Website
    c. Both

11. How important is data security and privacy for you when reporting an incident?
    a. Extremely important
    b. Important
    c. Neutral
    d. Not important

12. Have you ever used any technology or app to report incidents or seek help in emergencies (e.g., emergency response apps, neighborhood watch apps)?
    a. Yes
    b. No

13. Would you be willing to use SafeNet to report incidents and receive updates about public safety in your area?
    a. Yes
    b. No
    c. Maybe

14. Any additional feedback or suggestions to improve public safety services?

Stakeholders Feedback Summary: Based on the data collected through the various methods mentioned above, the following feedback was summarized from the key stakeholders:

- **Law Enforcement (Police Officers and Emergency Responders):**

  Priority Concerns: Quick access to incident details, real-time communication with citizens, and accurate location tracking for emergencies were highlighted as the most critical needs.
  Challenges: Current manual incident reporting processes often lead to delays in response times. Law enforcement officers also noted the need for an integrated system that works on both desktop and mobile devices.
  Feature Requests: Officers requested features like GPS-based tracking, alert systems, quick search options for criminal records, and integration with existing law enforcement databases. They also highlighted the need for data encryption and secure communication between the public and officers.

- **Healthcare Providers:**
  Priority Concerns: Easy and quick access to emergency contacts, real-time alerts about accidents, and collaboration with law enforcement during crisis situations.
  Challenges: Healthcare professionals often face delays due to a lack of real-time information on incidents, which impacts their ability to respond effectively.
  Feature Requests: Providers emphasized the need for integration with ambulance services, the ability to prioritize urgent cases, and the necessity for seamless communication between healthcare and law enforcement during emergencies.

- **Local Government Representatives:**

  Priority Concerns: Ensuring public safety, maintaining law and order, and improving collaboration between various departments such as health, police, and emergency services.
  Challenges: Disconnected systems between departments and inconsistent reporting of incidents were frequently cited.
  Feature Requests: Government stakeholders requested analytics and reporting tools to monitor incident trends, identify high-risk areas, and improve resource allocation.

- **General Public:**

  Priority Concerns: Simplified reporting processes, anonymity for sensitive cases, and fast response times from law enforcement were the top concerns for the public.
  Challenges: Citizens often find it difficult to report incidents due to complex systems, fear of exposure, or lack of clarity on the reporting procedure.
  Feature Requests: Users requested an easy-to-use mobile app with quick access to emergency services, live location sharing, push notifications for emergency alerts, and the ability to upload photos or videos as part of their reports.

User Requirements

1. User Identification and Verification

Requirement ID: UR-001

Description: Users must be able to verify the identity of police officers they interact with through the Police Identification Verification Feature.

Acceptance Criteria:

1. Users can input an officer's unique ID to check their identity.
2. The system must return the officer's name, police station, and verification status.
3. Verification results should be accessible within 30 seconds of input.

2. Emergency Service Locator

Requirement ID: UR-002

Description: Users must be able to locate the nearest police station or health center based on their current or specified location.

Acceptance Criteria:

1. Users can input or allow the platform to access their current location.
2. The system must display the nearest police stations and health centers, including name, address, contact number, and distance.
3. The system should provide a direct communication option (call, email, or message) to contact the nearest facility.

3. Officer Rating and Review

Requirement ID: UR-003

Description: Users must be able to rate and review their interactions with police officers to promote accountability and transparency.

Acceptance Criteria:

1. Users can submit ratings (1 to 5 stars) and written comments for each interaction.
2. The system must associate ratings and reviews with the correct officer based on their unique ID.
3. The system should calculate and display the average rating and reviews for each officer.
4. Users must be able to view and read reviews for any officer they wish to assess.

4. Anonymous Crime Reporting

Requirement ID: UR-004

Description: Users must be able to report crimes or suspicious activities anonymously through the platform.

Acceptance Criteria:

1. Users can submit reports without providing personal information.
2. The system must allow users to describe the incident and specify its location.
3. The report must be routed to the appropriate police station based on the location of the incident.
4. Users receive confirmation of submission and an incident reference number.

8. Notification and Feedback

Requirement ID: UR-008

Description: The platform must provide notifications and feedback to users regarding the status of their actions and reports.

Acceptance Criteria:

1. Users should receive notifications for successful report submissions, verification results, and review submissions.
2. Feedback on report processing and officer reviews should be timely and clear.
3. The platform should offer status updates for pending actions or issues.

Functional Requirements

1. Police Identification Verification Feature

Requirement ID: FR-001

Feature Description	Inputs	Outputs
This feature allows users to verify the identity of police officers through a unique ID system. Each officer is assigned a unique ID that can be verified via the platform to confirm their identity and police station affiliation.	=> Officer's Unique ID => Officer's Badge Number (optional) => Officer's Last Name (optional)	=> Officer's Full Name => Police Station Name => Verification Status => Officer's Profile Picture (if available)

Functional Requirements:

1. The system will allow officers to register their unique ID and related information on the platform.

2. The system will allow users to input an officer's unique ID for verification.

3. The system will check the validity of the ID against a database and return the officer's details.

4. The system will display a verification status indicating whether the officer is valid or invalid.

5. The system will provide feedback if the ID is invalid or not found.

2. Nearest Police Station & Health Center Locator Feature

Requirement ID: FR-002

Feature Description	Inputs	Outputs
This feature provides users with information about the nearest police stations and health centers based on their current location or a specified location. It includes contact details and direct communication options.	=> Current Location or Specified Location (address) => Type of Service Needed (Police Station/Health Center)	=>Nearest Police Station: - Name - Address - Contact Number - Distance from Current Location => Nearest Health Center: - Name - Address - Contact Number - Distance from Current Location

Functional Requirements:

1. The system will access location services to determine the user's current location or a specified address.

2. The system will provide a list of the nearest police stations and health centers based on the user's location. The view of the list priorities the nearest station/center.

3. The system will display detailed contact information and distance for each location.

4. The system will provide communication options to contact the nearest police station or health center.

3. Police Officer Rating and Review System Feature

Requirement ID: FR-003

Feature Description	Inputs	Outputs
This feature allows users to rate and review their interactions with police officers. It aims to maintain accountability, encourage positive behavior, and provide feedback for continuous improvement.	=> Officer's Unique ID => Case ID / Interaction ID => User Rating (1 to 5 stars) => Review Comments (text)	=> Average Rating for the Officer => User Reviews List => Aggregated Feedback Statistics

Functional Requirements:

1. The system will allow users to submit ratings and reviews for their interactions with police officers.

2. The system will require the input of the officer's ID to associate the review with the correct officer.

3. The system will allow users to provide a star rating and written comments.

4. The system will calculate and display the average rating for each officer.

5. The system will display a list of reviews and aggregate feedback statistics for each officer.

4. Anonymous Crime Reporting Feature

Requirement ID: FR-004

Feature Description	Inputs	Outputs
This feature allows users to report crimes or suspicious activities anonymously. The reports are sent directly to the appropriate police station based on the user's location.	=> Type of Incident (e.g., Crime, Suspicious Activity) => Description of the Incident => Location of the Incident	=> Confirmation of Report Submission => Incident Reference Number => Details of the Nearest Police Station Receiving the Report

Functional Requirements:

1. The system will allow users to submit crime or suspicious activity reports anonymously.

2. The system will accept details of the incident, including type, description, and location.

3. The system will route the report to the appropriate police station based on the incident location.

4. The system will provide confirmation of report submission, including an incident reference number.

5. The system will ensure that user anonymity is preserved and not disclosed to any parties.

Non- Functional Requirements

1. User Accessibility and Usability

Requirement ID: NFR-001

Description: The platform must be accessible and user-friendly across various devices & platform

Acceptance Criteria:

1. The platform should be compatible with major web browsers and mobile operating systems (iOS and Android).
2. The user interface must be intuitive and easy to navigate, with clear instructions and help options available.
3. The platform should provide accessibility features for users with disabilities, such as screen reader compatibility and adjustable text sizes.

2. Data Security and Privacy

Requirement ID: NFR-002

Description: The platform must ensure the security and privacy of user data, including anonymous reports and personal information.

Acceptance Criteria:

1. User data, including anonymous reports and personal information, must be encrypted and securely stored.
2. The platform should comply with relevant data protection regulations and privacy standards.
3. Access to sensitive data must be restricted to authorized personnel only, with proper authentication mechanisms in place.

3. System Performance and Reliability

Requirement ID: NFR-003

Description: The platform must perform reliably, with minimal downtime and fast response times.

Acceptance Criteria:

1. The system should be available 24/7.
2. Response times for user interactions and data retrieval should not exceed 5 seconds.
3. The system must handle high volumes of simultaneous users without significant degradation in performance.

Product Requirement

1. Purpose: SafeNet is designed to improve public safety by facilitating communication and collaboration between law enforcement agencies and the community. The platform aims to bridge the gap between citizens and police, enhance transparency, and promote accountability.

2. Product Functions:

SafeNet provides a variety of features that ensure reliable and effective communication between users and law enforcement:

- **Police Identification Verification:** Enables users to verify the identity of police officers in real-time.
- **Emergency Service Locator:** Provides users with details about the nearest police stations and health centers.
- **Officer Rating and Review System:** Allows citizens to rate and review their interactions with law enforcement officers.
- **Anonymous Crime Reporting:** Empowers users to report crimes or suspicious activities without revealing their identity.
- **Notifications and Feedback:** Keeps users informed about their interactions, reports, and system notifications.

3. Operational Environment:

SafeNet will be compatible with major operating systems (Android, iOS, Windows) and web browsers (Chrome, Firefox, Safari). The platform will be accessible via mobile apps and web browsers, optimized for both desktop and mobile usage.

4. Assumptions and Dependencies:

- Users have internet access to use the platform's features.
- The platform relies on integration with government databases (for police verification) and geolocation services (for emergency service locators).
- The platform must comply with data protection regulations, ensuring privacy and security for users and law enforcement agencies.

5. Performance Requirements:

SafeNet will ensure high performance with:

- Response Time: User interactions, such as police verification and emergency service locator results, should be displayed within 3-5 seconds.
- Scalability: The system should handle high volumes of users simultaneously without degrading performance.
- Availability: The platform should be operational 24/7, ensuring minimal downtime.

6. User Documentation:

- User Guide: Step-by-step instructions for citizens, police officers, and emergency health providers.
- FAQ Section: Addressing common issues and questions about platform usage.
- Support Contact Information: For users to seek help when facing issues.

System Requirements

1. Hardware Requirements: SafeNet requires a robust and scalable hardware infrastructure to ensure smooth operation for all users, including law enforcement and public citizens. The following are the minimum hardware requirements:

- **Server:**
  - RAM: 32 GB or higher
  - Storage: 2 TB SSD with redundancy
  - Backup: Cloud-based or on-premises backup with 4 TB storage capacity
  - Network Interface: Gigabit Ethernet (10/100 Mbps)

- **Client Devices (Police Stations, Health Centers, Public Access):**
  - Processor: Dual-core 2.0 GHz or higher
  - RAM: 4 GB or higher
  - Storage: 64 GB SSD or higher
  - GPS Module (for mobile units)

2. Software Requirements: SafeNet relies on specific software to manage operations and ensure system reliability. Below are the necessary software components:

- **Server Software:**
  - Operating System: Linux (Ubuntu 20.04 LTS or CentOS 8)
  - Web Server: Apache 2.4 or Nginx
  - Database: MySQL 8.0 or PostgreSQL 13
  - Programming Language: PHP 7.4 or higher, Python 3.8 for data processing
  - Application Framework: Laravel or Django for backend
  - Encryption: OpenSSL 1.1 or higher for secure communication
  - Logging and Monitoring: ELK stack (Elasticsearch, Logstash, Kibana)

- **Client Software (Web and Mobile):**
  - Web Browser: Google Chrome, Mozilla Firefox, Microsoft Edge (latest versions)
  - Mobile Operating System:
  - Android 8.0 or higher
  - iOS 13 or higher
  - Mobile Application: React Native or Flutter for cross-platform mobile app development
  - PDF Reader (for report generation and viewing)

3. Network Requirements: SafeNet’s performance depends on reliable and secure network connectivity. The system must ensure uninterrupted communication between users, law enforcement, and healthcare providers.

➢ **Network Protocols:**

- HTTP/2 for web communication
- Secure WebSocket (WSS) for real-time communication between users and law enforcement
- VPN support for secure access to internal systems
- Backup communication via SMS for users in areas with limited internet access
- Satellite communication (optional) for critical services in rural areas

4. Compatibility Requirements: SafeNet must be compatible across multiple platforms, devices, and operating environments to ensure widespread accessibility.

➢ **Operating System Compatibility:**

- Web: Compatible with Windows, Linux, and macOS operating systems
- Mobile: Must support Android (8.0 or higher) and iOS (13 or higher)
- Desktop: Compatible with Windows 10 and higher, macOS 10.15 and higher, and popular Linux distributions

➢ **Browser Compatibility:**

- Must be fully compatible with the latest versions of Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari
- Responsive design to ensure proper display on different screen sizes, from smartphones to desktop monitors

➢ **Mobile App Compatibility:**

- Cross-platform development for iOS and Android using frameworks such as React Native or Flutter
- Full support for GPS and location services
- Integration with mobile notification systems for emergency alerts

Requirement Analysis

Solve Conflict Requirement

CR 01: Law enforcement agencies prioritize detailed incident reports, while the general public prefers quick, anonymous reporting.
Resolution: Provide both options in the system. A detailed reporting option for law enforcement and a simplified, anonymous report option for the public.

CR 02: Healthcare centers require access to sensitive health data during emergencies, but local government representatives and the general public emphasize privacy concerns.
Resolution: Implement a role-based access control system that grants healthcare centers access to sensitive data only when authorized, while maintaining strict privacy controls for the general public.

CR 03: Law enforcement requires real-time data from all locations, while local government representatives suggest focusing on certain high-risk areas first due to limited resources.
Resolution: Implement a phased rollout of real-time data access, starting with high-risk areas and expanding as resources permit, with customizable settings for each region.

Prioritization

- **High Priority:**
  - Real-time incident reporting with GPS location
  - Quick and anonymous reporting option for the public
  - Secure communication with law enforcement
  - Role-based access control for sensitive data (e.g., healthcare emergencies)
  - Alerts for emergencies in specific areas

- **Medium Priority:**
  - Emergency contact registration
  - Detailed incident reports for law enforcement
  - Integration with local government databases for infrastructure-related emergencies
  - In-app feedback and follow-up on reported incidents

- **Low Priority:**
  - Public safety tips and awareness campaigns
  - Customizable dashboard for different user types (public, law enforcement, healthcare)

Requirement Validation

Requirement validation ensures that the requirements gathered for the SafeNet platform are correct, complete, and aligned with stakeholder expectations. The process involves verifying the functionality, usability, and overall user experience by creating mock-ups, wireframes, prototypes, and a detailed user interface (UI). These tools help stakeholders visualize the system before full development.

Mock-Up: A mock-up is a static high-fidelity visual representation of the user interface, focusing on the design and layout of the system. It demonstrates how the system will look once developed. The mock-up is useful for quickly validating the visual aspects of the SafeNet platform with stakeholders such as law enforcement, healthcare centers, local government representatives, and the general public.

Wireframe: A wireframe is a low-fidelity visual representation that outlines the structure and functionality of the platform without focusing on design details. Wireframes are primarily used to show how the various features and sections of the SafeNet platform will be organized, including navigation flow and functional layout. For wireframes, additional files will be attached with SRS Template.

Prototype: A prototype is a working model of the platform that incorporates both visual and functional elements. It allows stakeholders to interact with the system in a limited manner, simulating real user flows and actions. Prototypes can be low- or high-fidelity and help in testing how well the system meets user requirements.

By using mock-ups, wireframes, prototypes, and detailed UI designs during the Requirement Validation phase, stakeholders can visualize the SafeNet platform, provide feedback, and ensure that their needs are met before the development process. This proactive validation reduces the risk of misunderstandings or missing features and ensures that the platform aligns with user expectations and business objectives.

Finalize Requirement

The Finalize Requirement phase ensures that all requirements for the SafeNet platform are clearly defined, validated, and ready for implementation. This phase includes a thorough review of the gathered requirements, defect checking to identify any inconsistencies or gaps, and establishing testing criteria to ensure the platform meets both functional and non-functional expectations.

Reviewing Requirements: In this step, all previously gathered and analyzed requirements are revisited to ensure completeness, clarity, and alignment with stakeholder needs. The review process involves multiple stakeholders, including law enforcement agencies, healthcare centers, local government representatives, and the general public.

- **Steps in Reviewing Requirements:**
  - Cross-Checking with Stakeholders: Ensure that all identified features, functionalities, and constraints have been agreed upon by all stakeholders.
  - Consistency Check: Ensure that there are no contradictions or inconsistencies in the requirements.
  - Traceability Matrix: Create a traceability matrix to ensure that each requirement can be traced back to its original source (e.g., user needs, business rules).
  - Feasibility Analysis: Verify the technical and operational feasibility of each requirement.

- **Outcomes of Review:**
  - Ensure that all functional, non-functional, and business requirements are well-defined.
  - Confirm that all stakeholders agree with the final requirements.
  - Identify any potential risks that may arise during implementation.

Defect Checklist: The Defect Checklist helps identify any issues or ambiguities in the requirements before they are passed on for development. It is a structured list used to evaluate the quality of the requirements.

- **Defect Checklist Includes:**
  1. Completeness: Are all the requirements fully documented? Is there any missing information?
  2. Clarity: Are the requirements clearly stated without any ambiguities?
  3. Consistency: Do the requirements conflict with each other or other parts of the project?
  4. Testability: Can the requirements be easily tested to ensure they are correctly implemented?
  5. Feasibility: Are the requirements technically feasible within the given time and budget?
  6. Traceability: Are all requirements traceable to their original stakeholder or source?
  7. Prioritization: Are the requirements prioritized according to their importance and impact?
  8. Performance: Are performance-related requirements specified (e.g., speed, capacity)?
  9. Security: Are there requirements addressing the security of the platform, including data protection and user privacy?
  10. Usability: Are the user interface and user experience (UI/UX) requirements clearly defined?

- **Outcome:**
  - Ensures that all defects are identified and resolved before development begins.
  - Guarantees that the SafeNet platform's requirements are of high quality and free of ambiguity or conflict.

Testing Requirement: The Testing Requirement phase focuses on defining how each requirement will be validated during the testing phase. It involves creating test cases for each requirement to ensure that the system functions as intended once it is developed.

- **Testing Strategies:**
  - Unit Testing: Test individual components of the platform to ensure they function correctly in isolation (e.g., incident reporting, user registration).
  - Integration Testing: Ensure that different modules of the platform (e.g., law enforcement and healthcare modules) work together seamlessly.
  - System Testing: Validate that the entire SafeNet platform works as a cohesive system, meeting both functional and non-functional requirements.
  - User Acceptance Testing (UAT): Allow stakeholders, including law enforcement and healthcare representatives, to test the platform to ensure it meets their needs and expectations.
  - Security Testing: Ensure the platform is secure from unauthorized access and data breaches, as it handles sensitive public information and law enforcement data.
  - Performance Testing: Measure the platform's performance under various conditions to ensure it meets speed, load, and scalability requirements.

- **Testing Criteria:**
  - Functional Requirements: Ensure that all the platform's features (e.g., incident reporting, law enforcement response tracking) function correctly.
  - Non-Functional Requirements: Validate performance (e.g., response times), security (e.g., data encryption), usability (e.g., user-friendly interface), and compatibility (e.g., cross-platform functionality).
  - Error Handling: Confirm that the system gracefully handles errors, providing clear feedback to users without compromising the system.
  - Data Validation: Ensure that all user input is validated, reducing the risk of invalid or malicious data entry.

- **Outcome:**
  - Clearly defined testing requirements ensure that all aspects of the SafeNet platform can be tested thoroughly.
  - This phase ensures that the system meets the expected standards and requirements before launch.

Appendix

The appendix provides supplementary information that supports the understanding of the SRS document. It includes definitions, acronyms, and any additional materials that help clarify the requirements specified within the document.

- **Glossary of Terms**
  1. **Law Enforcement Agency:** Any government organization that enforces laws and maintains public order and safety (e.g., police departments).
  2. **Healthcare Center:** A facility where medical services are provided to individuals.
  3. **Local Government Representative:** Officials from local governing bodies responsible for managing specific regional or municipal functions.
  4. **General Public:** The individuals within the community who interact with the SafeNet platform and report incidents or emergencies.
  5. **SafeNet:** A public safety platform designed to enhance communication between citizens and law enforcement and provide timely access to emergency services.
  6. **Stakeholders:** Individuals or organizations with an interest in the development and outcome of the SafeNet platform (e.g., government, police, healthcare centers).
  7. **Requirement Elicitation:** The process of gathering and understanding requirements from stakeholders to develop a system that meets their needs.
  8. **Mock-Up:** A static visual representation of the system’s interface used for validation & feedback.
  9. **Wireframe:** A basic visual guide used to suggest the structure and relationships between elements in the system.
  10. **Prototype:** A working model of the system used to simulate and test certain functionalities before full development.
  11. **User Interface (UI):** The visual layout through which users interact with the SafeNet platform.
  12. **SRS:** Software Requirements Specification, a document that defines the system’s intended features, functionalities, and constraints.

- **Acronyms**
  1. **SRS**: Software Requirements Specification
  2. **UI**: User Interface
  3. **UAT**: User Acceptance Testing
  4. **SLR**: Systematic Literature Review
  5. **API**: Application Programming Interface
  6. **HTTP**: Hypertext Transfer Protocol
  7. **CRUD**: Create, Read, Update, Delete
  8. **SSL**: Secure Sockets Layer
  9. **JSON**: JavaScript Object Notation
  10. **MVC**: Model-View-Controller (architecture pattern for building applications)

Acknowledgements

- **Software Requirements by Karl Wiegers, Joy Beatty** (for providing foundational knowledge and best practices essential for developing this document)
- **ChatGPT** (for its crucial assistance in refining the SRS document through insightful guidance and support)