**Project Title: Face Recognition System**

**Business Requirement Document**

|  |  |
| --- | --- |
| **Author Name:** | **Jayasuriya J** |
| **Date:** |  |
| **Version:** | **1.1** |
| **Status:** | **In Progress** |

# Table of Contents

1. Introduction ……………………………………………………………………………………………………………*03*

1.1 Project Overview …………………………………………………………………………………………………...*03*

1.2 Purpose …………………………………………………………………………………………………………………*03*

1.3 Scope ……………………………………………………………………………………………………………………*03-04*

1.4 Definitions, Acronyms, and Abbreviations ……………………………………………………………*04-05*

2. Business Objectives ……………………………………………………………………………………………….*05*

3. Stakeholders ………………………………………………………………………………………………………....*05*

3.1 Stakeholder Identification ……………………………………………………………………………………*05-06*

3.2 Stakeholder Roles and Responsibilities ……………………………………………………………….*06-08*

4. Requirements ……………………………………………………………………………………………………….*08*

4.1 Functional Requirements …………………………………………………………………………………….*08-14*

4.2 Non-Functional Requirements …………………………………………………………………………….*14-15*

5. Assumptions and Constraints …………………………………………………………………………………*15*

6. Glossary …………………………………………………………………………………………………………………*16*

7. Approval …………………………………………………………………………………………………………………*16*

7.1 Sign-Off ………………………………………………………………………………………………………………….*16*

**1.Introduction**

## **1.1 Project Overview**

Our Face Recognition System (FRS) is designed to provide fast, accurate, and secure identification in workplaces. It works in any lighting condition and recognizes faces from different angles, eliminating errors in traditional systems. With real-time attendance tracking and AI-driven security features, it improves efficiency and prevents unauthorized access. FRS seamlessly integrates with existing security systems, making it ideal for corporate, retail, and industrial environments. Future enhancements include emotion detection, voice recognition, and cloud-based processing for smarter operations.

## **1.2 Purpose**

The Face Recognition System (FRS) is built to automate attendance tracking and improve security in workplaces. It eliminates manual errors, long wait times, and unauthorized access by using AI-powered facial recognition. With fast, contactless identification and anti-spoofing technology, FRS ensures efficient workforce management and secure access control for businesses.

## **1.3 Scope**

**In scope:**

* **Face Detection & Recognition** – The system accurately identifies people in real-time using AI. It works even if the person is moving or not directly facing the camera.
* **Attendance Tracking** – FRS automates attendance marking, removing the need for manual check-ins. This reduces waiting time and eliminates human errors.
* **Multi-Angle Recognition** – The system recognizes faces even if they are slightly turned or tilted. Users don’t need to adjust their positions for detection.
* **Low-Light Recognition** – FRS works even in dim lighting, ensuring reliable recognition in all conditions. This makes it useful for offices, factories, and retail spaces.
* **Access Control** – Only authorized individuals can enter restricted areas. The system enhances security by preventing unauthorized access.
* **Integration with Security Systems** – FRS can connect with existing security setups like smart locks and CCTV. This improves monitoring and overall safety.
* **Real-Time Monitoring** – The system tracks attendance and movement instantly. Managers can check live updates and reports anytime.
* **Anti-Spoofing Technology** – FRS prevents fraud by detecting fake photos, videos, or masks. This ensures that only real individuals are recognized.

**Out of Scope**

* **Fingerprint or RFID-Based Attendance** – The system only uses face recognition, not fingerprints or ID cards. It focuses on a contactless experience.
* **Offline Functionality** – FRS needs an internet or network connection to process and verify faces. It won’t work in offline mode.
* **Emotion Detection & Voice Recognition** – The system does not detect emotions or recognize voices in this version. These features are planned for future updates.
* **Personal Data Storage** – FRS does not store sensitive personal details beyond identification. It only keeps the minimum data required for recognition.
* **Standalone Hardware Development** – The system is software-based and works with existing cameras. It does not involve developing new hardware devices.

## **1.4 Definitions, Acronyms, and Abbreviations**

**Definitions:**

* **End User** – The person who will use the Face Recognition System (FRS) for attendance, security, or access control. This could be employees, security staff, or system administrators.
* **Facial Recognition** – A technology that scans and identifies a person’s face using AI, without needing physical contact.
* **Access Control** – A security feature that ensures only authorized individuals can enter a location or system.
* **Anti-Spoofing** – A protection mechanism that prevents fake attempts like using photos or videos to trick the system.
* **Real-Time Monitoring** – The ability to track attendance and security updates instantly, without delays.

**Acronyms:**

**FRS** – Face Recognition System  
**AI** – Artificial Intelligence  
**BRD** – Business Requirement Document  
**UI/UX** – User Interface/User Experience  
**RTM** – Requirement Traceability Matrix  
**API** – Application Programming Interface (Used for integration with other systems)

**Abbreviations:**

**OTP** – One-Time Password (Used for multi-factor authentication)  
**DB** – Database (Where facial recognition data is stored securely)  
**CAM** – Camera (Used to capture real-time facial images)  
**ID** – Identification (Unique details used for recognizing a person)

# **2. Business Objectives**

The Face Recognition System (FRS) is designed to automate attendance and improve security in workplaces. It eliminates manual errors, long wait times, and unauthorized access by using AI-powered facial recognition. Businesses can save time, increase efficiency, and enhance security with real-time monitoring. FRS also integrates with existing security systems for seamless access control. Future upgrades will include emotion detection, voice recognition, and cloud-based processing to make it even smarter.

**3.Stakeholders**

**3.1 Stakeholders Identification**

* **Business Owners** – They provide the funding and make key decisions to ensure the project aligns with the company’s vision and goals.
* **Subject Matter Experts (SMEs)** – Experts in AI, security, and biometrics who provide insights on how FRS should function and meet industry standards.
* **Business Analyst** – Gathers requirements from different stakeholders, ensures all needs are documented, and translates them into clear project goals.
* **Developers** – Responsible for building the FRS software, coding the AI recognition system, and ensuring smooth functionality across all features.
* **QA Team (Quality Assurance)** – Tests the system to find and fix bugs, making sure FRS works accurately in different conditions before launch.
* **UI/UX Designers** – Design the interface to make the system easy to use, ensuring smooth navigation for both admins and end users.
* **IT & Security Team** – Handles system integration, cybersecurity, and data protection to prevent unauthorized access and maintain privacy.
* **HR Team** – If FRS is used for attendance tracking, HR teams will rely on it for payroll and workforce management.
* **Operations Manager** – Ensures smooth implementation and daily operations, especially in high-traffic areas like offices or factories.
* **Compliance & Legal Team** – Ensures FRS follows data privacy laws and industry regulations (GDPR, IT Act, etc.).
* **System Administrators** – Manage the backend, handle user access, and troubleshoot any technical issues.
* **End Users** – Employees, security personnel, and management teams who will use FRS daily for attendance tracking and access control.

## **3.2 Stakeholder Roles and Responsibilities**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Name** | | |  | | --- | | **Role** | | |  | | --- | | **Responsibilities** | | |  | | --- | | **Email ID** | |
| Vinoth | Business Owner | Provides funding, sets strategic goals, and ensures project success. | vinoth@gmail.com |
| Subhapriya | Subject Matter Expert (SME) | Offers expertise in AI, biometrics, and security for FRS development. | subhapriya@gmail.com |
| Jayasuriya | Business Analyst | Gathers and documents requirements, ensuring alignment with business needs. | Jsuriya454@gmail.com |
| Subha | Lead Developer | Develops the core FRS system, writes AI recognition algorithms, and ensures system functionality. | subha@gmail.com |
| Dinesh | QA Tester | Tests FRS for accuracy, detects bugs, and ensures it works in different environments. | dinesh42@gmail.com |
| Danush | UI/UX Designer | Designs an intuitive and user-friendly interface for both admins and users. | danush1@gmail.com |
| Dhanush | IT & Security Specialist | Manages cybersecurity, system integration, and ensures data privacy compliance. | dhanush@gmail.com |
| Vasumathi | HR Manager | Uses FRS for employee attendance tracking and workforce management. | vasu@gmail.com |
| Madhumathi | System Administrator | Handles backend operations, manages user access, and troubleshoots technical issues. | madhu@gmail.com |
| Vignesh | Operations Manager | |  | | --- | | Oversees system deployment and ensures smooth functioning in different locations. |  |  | | --- | |  | | vignesh@gmail.com |
| Kishore | Compliance & Legal Officer | Ensures FRS follows legal and industry regulations on data protection and privacy. | kishore@gmail.com |
| Selvaganesh | Employees & Security Staff | Use FRS for attendance and access control, providing feedback for improvements. | selvaganesh@gmail.com |

# **4. Requirements**

## **4.1 Functional Requirements**

**Requirement 1: User Registration**

**Title:** User Registration  
  
**Description:** Users need to register their details and facial data to access the system.  
  
**Assumptions:**

* Users have a valid email ID and a working camera for facial registration.
* The system securely stores facial recognition data.

**Dependencies:**

* Internet connection for online registration.
* Database to store user details and facial features.

**Preconditions:**

* The user must provide necessary details like name, email, and face scan.

**Postconditions:**

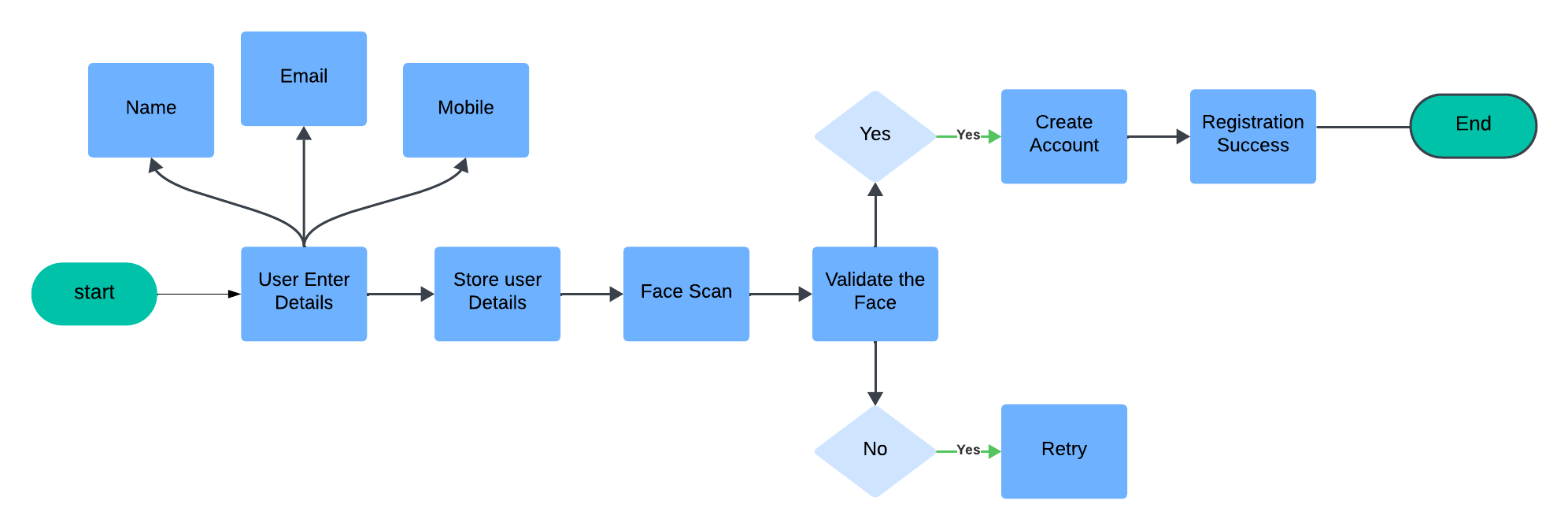
* The user is successfully registered and stored in the system.
* The system generates a unique ID for the user.

**Acceptance Criteria:**

* The system must verify and store the user’s facial data securely.
* Registration should be completed within **5 seconds**.
* If an error occurs, an appropriate message must be displayed.

**Priority:** High

**Process Flow Diagram:**



**Requirement 2: User Login with Face Recognition**

**Title:** Face Recognition Login  
  
**Description:** Users can log in by scanning their face instead of using a password.  
  
**Assumptions:**

* Users have registered in the system.
* The camera is functional and clear.

**Dependencies:**

* User Registration functionality.
* AI-based face matching algorithm.

**Preconditions:**

* The user must be registered in the system.
* The camera must be active for scanning.

**Postconditions:**

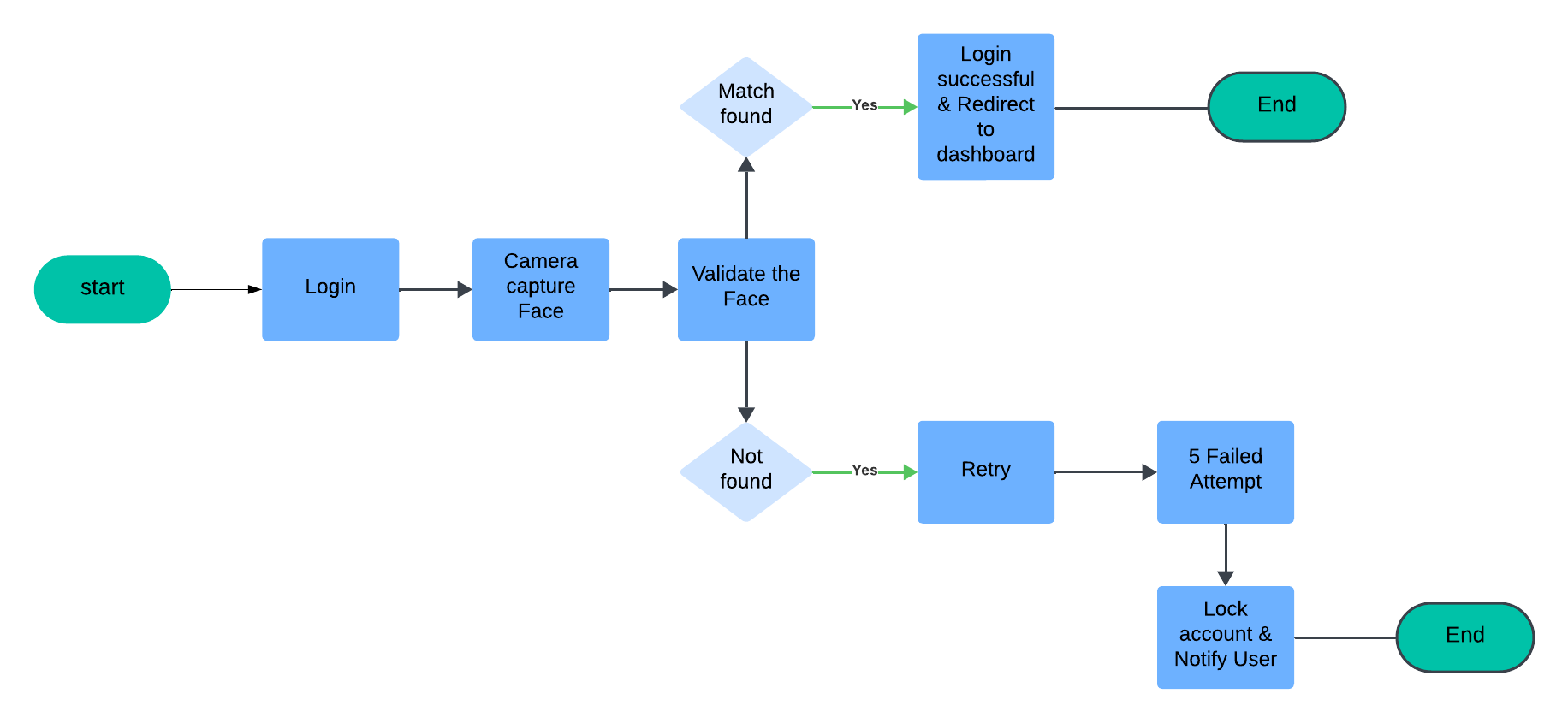
* The user is successfully logged in and redirected to the dashboard.
* The login time and IP address are recorded.

**Acceptance Criteria:**

* The system must recognize the user’s face within **2 seconds**.
* If face authentication fails, an error message is shown.
* After **5 failed attempts**, the system locks the user’s account.

**Priority:** High

**Process Flow Diagram:**

****

**Requirement 3: Attendance Tracking**

**Title:** Automated Attendance Tracking  
  
**Description:** The system records attendance automatically when a registered face is detected.  
  
**Assumptions:**

* Users are physically present during attendance marking.
* The camera and AI detection are working correctly.

**Dependencies:**

* Face Recognition Login.
* Attendance report module.

**Preconditions:**

* The user must be registered in the system.

**Postconditions:**

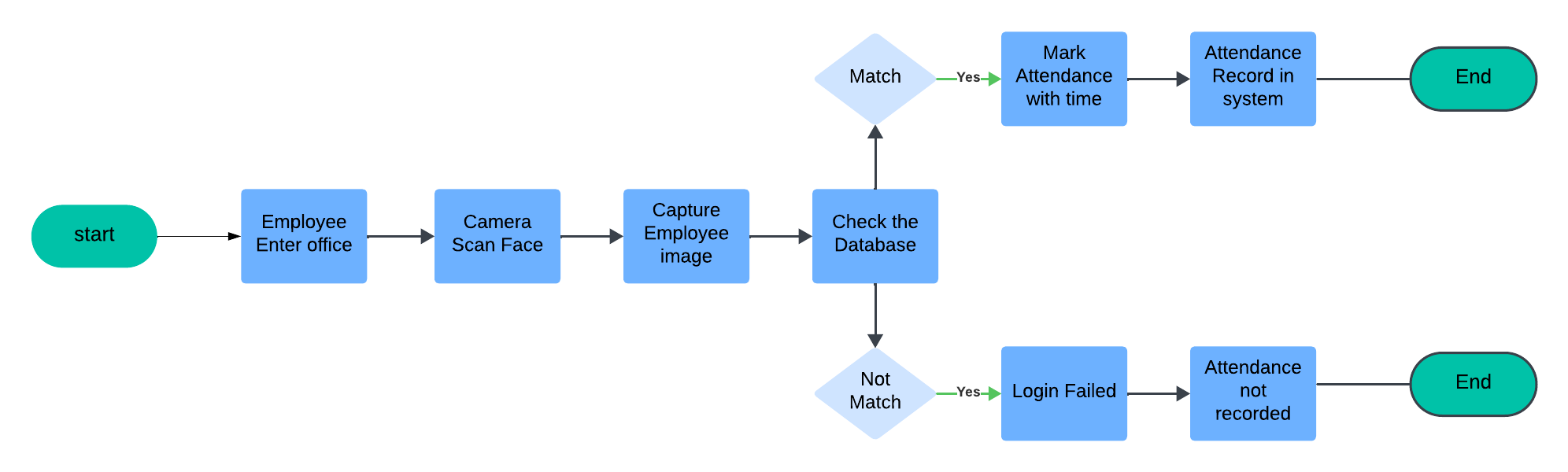
* Attendance is marked successfully with a timestamp.
* Data is stored for reporting purposes.

**Acceptance Criteria:**

* Attendance is recorded within **2 seconds** of face detection.
* If the system fails to detect a face, an error is logged.
* Users receive a confirmation message after attendance is marked.

**Priority:** High

**Process Flow Diagram:**



**Requirement 4: Security and Anti-Spoofing**

**Title:** Security & Anti-Spoofing  
  
**Description:** The system prevents unauthorized access using AI-driven security checks.  
  
**Assumptions:**

* Users are real individuals and not using fake images or videos.

**Dependencies:**

* Face Recognition Login.
* AI-powered spoof detection.

**Preconditions:**

* The user must be physically present for authentication.

**Postconditions:**

* Fake attempts (using photos/videos) are detected and blocked.
* Unauthorized access attempts are logged.

**Acceptance Criteria:**

* The system must detect and reject spoofing attempts within **2 seconds**.
* If fraud is detected, an alert is sent to the admin.
* The system must log all unauthorized attempts.

**Priority:** High  
  
**Process Flow Diagram:**

A diagram of a system

AI-generated content may be incorrect.

## **4.2 Non-Functional Requirements**

**Performance**

* The system should return search results within 2 seconds for a smooth user experience. Login authentication must be processed in under 5 seconds under normal conditions. The system should handle high traffic without slowdowns.

**Usability**

* The interface must be simple, intuitive, and accessible across devices. Form fields should provide clear error messages for incorrect inputs. The system must follow WCAG 2.1 accessibility standards for inclusivity.

**Security**

* User passwords must be securely hashed using strong algorithms like bcrypt. Data must be encrypted in transit and at rest to prevent breaches. Multi-factor authentication (MFA) should be supported for extra security.

**Scalability**

* The system must support 50,000 concurrent users without performance issues. It should allow horizontal scaling to accommodate future growth. Database queries must be optimized for fast data retrieval.

**Compliance**

* The platform must follow GDPR, CCPA, and relevant data laws to protect user privacy. User consent should be obtained before storing personal data. Regular security audits must be conducted to ensure compliance.

**Interoperability**

* The system must integrate smoothly with third-party services like Google Maps and payment gateways. APIs should follow RESTful architecture for easy integration. The application must work flawlessly on all major browsers.

# **5. Assumptions and Constraints**

**Assumptions:**

* **System Availability:** Servers and network infrastructure will be stable and accessible at all times.
* **User Knowledge:** Users have basic digital literacy to navigate the system without extensive training.
* **Third-Party Services:** External APIs (e.g., Google Maps) will remain operational and compatible.

**Constraints:**

* **Budget:** The project must be completed within ₹12,50,000 without exceeding costs.
* **Timeline:** The system must be fully developed and deployed within five months.
* **Technology Stack:** The project must use Python, React, and PostgreSQL as core technologies.
* **Data Privacy:** The system must comply with GDPR and CCPA for secure user data handling.

**Glossary:**

* **FRS:** A document outlining the functional requirements of a system.
* **API:** A set of rules that allow different software systems to communicate.
* **Latency:** The time it takes for a system to respond to a user request.
* **Encryption:** The process of securing data to prevent unauthorized access.
* **User Experience (UX):** The overall experience of a person using the system.

# **7. Approval**

## **7.1 Sign-Off**

**Vinoth  
Business Owner**