1. Introduction

1.1 Purpose of the Document

The purpose of this Software Requirements Specification (SRS) is to outline and describe the **Minimum Viable Product (MVP)** for the Cybercrime Prevention Platform. It details the system's functional and non-functional requirements, user roles, constraints, and dependencies. This document provides a clear reference for the development team, stakeholders, and future maintenance efforts.

1.2 Intended Audience

- **Development Team**: To understand the project scope, requirements, and functionalities.
- **Project Stakeholders**: Project sponsors, hackathon judges, or business owners who need a comprehensive overview of the system.
- **Quality Assurance (QA) Team**: To develop test cases aligned with the specified requirements.
- **Legal & Cybersecurity Consultants**: To ensure the system meets legal standards and adequately addresses cybersecurity needs.

1.3 Scope

The MVP will allow users to:

- **Upload and analyze documents** (e.g., Terms & Conditions) using LLM to identify risks and compliance gaps.
- **Check phishing links** and suspicious files.
- **Check for spam IP addresses** via integrated threat intelligence sources.
- **Verify password leaks** via known breach repositories.
- **View or request legal assistance** from a lawyer marketplace.
- **Handle user authentication** (login, signup) and provide an **admin panel** for Lawyer CRUD operations.

This system is primarily web-based, with potential for future expansions (e.g., browser extensions, advanced threat detection, dark web scans). For now, we focus on essential back-end APIs, front-end interfaces, and minimal but crucial business logic for a successful demonstration.

1.4 Definitions, Acronyms, and Abbreviations

- **LLM**: Large Language Model
- **RAG**: Retrieval-Augmented Generation

- **CRUD**: Create, Read, Update, Delete
- **API**: Application Programming Interface
- **MFA**: Multi-Factor Authentication
- **T&C**: Terms & Conditions
- **UI**: User Interface
- **PDF**: Portable Document Format
- **MVP**: Minimum Viable Product

2. Overall Description

2.1 Product Perspective

This platform is a new, stand-alone web-based solution that integrates:

1. **Open-source LLM** for document analysis and Q&A.
2. **Cybersecurity APIs** (phishing link checks, IP reputation checks, password leak checks) for robust threat detection.
3. **Marketplace module** for connecting users with lawyers specializing in cybercrime issues.

2.2 Product Features

1. **Document Analysis**: Users can upload documents (PDFs, text files) and receive legal/compliance insights.
2. **Cybersecurity Tools**: Phishing link detector, IP spam detector, password leak checker.
3. **Authentication Module**: User signup and login with basic password strength checks.
4. **Admin Panel**: Manages lawyer profiles via CRUD operations.
5. **Lawyer Marketplace**: View and contact listed lawyers for further legal assistance.
6. **Multi-language Support**: Toggle between Nepali and English (with potential expansion for more languages).

2.3 User Classes and Characteristics

1. **End User** (Individual or Corporate Employee)
    - Needs to upload documents for legal/compliance checks.
    - Requires quick phishing and spam detection.
    - Wants to check if credentials are compromised.
2. **Admin**
    - Manages lawyer profiles and platform content.
    - Views usage statistics (optional in MVP).

3. **Lawyer**
    - Listed on the marketplace for user consultation.
    - Profile management (optional if not handled by admin in the MVP).

2.4 Operating Environment

- **Web-based application** accessible via modern browsers (Chrome, Firefox, Safari, Edge).
- **Server environment**: Cloud-based or on-premise server running the back-end (Node.js, Python, or other frameworks) with Docker/virtual environment support.
- **Database**: PostgreSQL, MySQL, or MongoDB for storing user data, lawyer profiles, and minimal logs.

2.5 Design and Implementation Constraints

- **Integration with External APIs**: Must be able to consume phishing, IP reputation, and password leak APIs.
- **LLM Resource Usage**: Ensure minimal latency; may require GPU/CPU optimization or caching for fast responses.
- **Security**: Must handle user credentials securely (hashing, salted passwords, recommended encryption).
- **Legal Considerations**: Must display disclaimers that the LLM's legal/compliance advice is not a substitute for a licensed lawyer.

2.6 Assumptions and Dependencies

- Users have stable internet access.
- External APIs are reliable and have predictable response times.
- There is a valid SSL certificate for secure communication.
- Data breach repositories and threat intelligence feeds remain public or have accessible APIs.
- LLM model and RAG approach can handle multi-language toggling (Nepali/English).

3. Specific Requirements

3.1 Functional Requirements

3.1.1 User Authentication

FR-1.1: The system shall provide **signup** functionality, requiring:

- Username or email

- Password (meeting strength criteria)

FR-1.2: The system shall provide **login** functionality.
FR-1.3: (Optional for MVP) The system may provide **password reset** or recovery functionality.
FR-1.4: (Optional for MVP) The system may support **Multi-Factor Authentication (MFA)**.

3.1.2 LLM-Powered Document Analysis

FR-2.1: The system shall allow users to **upload documents** (PDF, text).
FR-2.2: The system shall process the document through the **open-source LLM** for:

- Risk detection (e.g., suspicious clauses in T&C).
- Basic compliance check (e.g., highlights sections relevant to data protection regulations).
- Summary of key legal points.

FR-2.3: The system shall **store** or **cache** analyzed results (up to an MVP-defined limit, e.g., last 5 documents).
FR-2.4: The system shall **display** analysis results in a clear user interface.

3.1.3 Cybersecurity Tools

1. **Phishing Link Detector**
    - **FR-3.1**: Users can **input a URL** and receive an immediate safety check (API-based or local ML model).
    - **FR-3.2**: The system shall return a **risk level** (Safe, Suspicious, Malicious) and brief explanation.
2. **Phishing File Detector**
    - **FR-3.3**: Users can **upload a file** (PDF, Doc) to scan for embedded phishing links or macros.
    - **FR-3.4**: The system shall **flag** files containing suspicious URLs or known malicious signatures.
3. **Spam IP Detector**
    - **FR-3.5**: Users can **input an IP address** to check if it is flagged for spam or malicious activity.
    - **FR-3.6**: Results shall be displayed with a short explanation and threat score if available.
4. **Password Leak Checker**
    - **FR-3.7**: Users can **input an email/username** to see if it appears in known data breaches.
    - **FR-3.8**: The system shall **inform** users if the email/username was found, with references to the breach data (if available).

3.1.4 Multi-language Support

FR-4.1: The system shall allow users to **toggle** between Nepali and English for the user interface.

FR-4.2: The system shall **pass** user language preference to the LLM to **generate content** in the requested language.

3.1.5 Marketplace (Lawyer Profiles)

FR-5.1: The system shall display a list of **lawyer profiles** (e.g., name, specialization, contact info).
FR-5.2: The system shall allow an **admin** to **create, read, update, and delete** lawyer entries.
FR-5.3: (Optional for MVP) End-users can **request** or **schedule** a consultation with a listed lawyer.

3.1.6 Admin Panel

FR-6.1: The system shall provide an **admin dashboard** to:

- Manage lawyer profiles (CRUD).
- (Optional) View basic usage stats (e.g., number of documents analyzed).

FR-6.2: Admin users must be **authenticated** (admin role) to access the dashboard.

3.2 Non-Functional Requirements

3.2.1 Performance

- **NFR-1.1**: The platform should respond to standard queries (e.g., phishing link checks) within **2 seconds** on average.
- **NFR-1.2**: Document analysis should complete within **5-10 seconds** for documents under 5 MB, subject to server and LLM constraints.

3.2.2 Security

- **NFR-2.1**: All data in transit must be **encrypted** via HTTPS.
- **NFR-2.2**: User passwords should be **hashed** using a secure hashing algorithm (e.g., Argon2, bcrypt).
- **NFR-2.3**: The system should follow **role-based access control (RBAC)** for admin vs. regular users.
- **NFR-2.4**: The system must have **proper input validation** to mitigate injection attacks.

3.2.3 Usability

- **NFR-3.1**: The user interface should be **intuitive** and require minimal technical knowledge for standard actions (uploading files, checking URLs).
- **NFR-3.2**: Users should be able to toggle languages (Nepali/English) with **one click** and see changes immediately.

3.2.4 Reliability & Availability

- **NFR-4.1**: The system should be available **99%** of the time during the MVP phase.
- **NFR-4.2**: Critical services (authentication, phishing detection) should handle **graceful degradation** if external APIs fail.

3.2.5 Maintainability

- **NFR-5.1**: The system's architecture should separate **frontend, backend, and external APIs** for easier updates and maintenance.
- **NFR-5.2**: The codebase should follow **standard design patterns** and **well-documented** modules.

3.3 External Interface Requirements

3.3.1 User Interface

- A **responsive web** UI that supports desktops, tablets, and smartphones.
- Key screens: Home (landing page), Login/Signup, Document Upload, Cybersecurity Tools Dashboard, Admin Panel, Marketplace.

3.3.2 Hardware Interfaces

- No specialized hardware required beyond standard computing devices with an internet connection.

3.3.3 Software Interfaces

1. **Operating System**: Independent (Windows, macOS, Linux).
2. **Browsers**: Latest versions of Chrome, Firefox, Safari, Edge.
3. **APIs**:
    - Phishing detection service (3rd-party or in-house).
    - IP reputation service.
    - Password breach database (e.g., Have I Been Pwned or similar).
    - LLM service (self-hosted or remote inference endpoint).

3.3.4 Communication Interfaces

- **HTTPS** for all data exchanges between client and server.
- **RESTful APIs** for internal or external integrations.

4. Other Requirements

4.1 Legal and Regulatory Requirements

- System must present **disclaimers** clarifying that LLM advice is non-binding and users should consult a qualified lawyer for final opinions.
- Comply with basic **data privacy** standards; gather only essential user information and store it securely.

4.2 Documentation

- **User Guide**: Quick start instructions for end-users and admin users.
- **API Documentation** (if relevant for external or internal integrators).
- **Developer Documentation**: Basic guidelines on setting up the local environment and deploying to production.

4.3 Future Enhancements (Post-MVP)

- **Advanced Threat Intelligence**: Integration with real-time threat feeds, advanced ML for malware detection.
- **Browser Extension** for phishing link checks.
- **Dark Web Monitoring** to detect stolen credentials.
- **Video & Image Analysis**: Extended for deepfake detection, suspicious patterns, etc.

5. Appendix or References

1. **IEEE 830-1998** – Recommended Practice for Software Requirements Specifications.
2. **External APIs** – Documentation links for phishing, IP reputation, and password breach services.
3. **LLM References** – Documentation for the open-source LLM being utilized, plus instructions for RAG integration.