# SOFTWARE REQUIREMENTS SPECIFICATION

## for

# CYBERCRIME INCIDENT MANAGEMENT & AWARENESS SYSTEM (CIMAS)

**Version 1.0**

**Prepared by :**
**1. Adithayan AS (4)**
**2. Adwin T Sunil (5)**
**3. Evaan Antony Philip (23)**

**September 20, 2025**

# Contents

# 1 Introduction

## 1.1 Purpose

Cybercrime is a growing threat worldwide, and managing incidents effectively is a major challenge. The purpose of the Cybercrime Incident Management & Awareness System (CIMAS) is to provide a secure, centralized platform where victims can report incidents, submit evidence, and track the status of their cases. Investigators and authorities can assign, monitor, and manage cases more efficiently. Additionally, CIMAS includes an Awareness Hub that educates the public about safe online practices.

## 1.2 Intended Audience and Reading Suggestions

This SRS is intended for developers, cybersecurity professionals, law enforcement authorities, project managers, and testers. It provides details on both functional and non-functional requirements of CIMAS, ensuring clarity for implementation, deployment, and evaluation.

## 1.3 Project Scope

CIMAS is designed to streamline the process of reporting and investigating cybercrime cases. Key objectives include:

- Enabling victims to securely report incidents with supporting evidence.
- Allowing investigators to track, assign, and manage cases.
- Offering data-driven insights through crime mapping and analytics.
- Providing an Awareness Hub to educate the public on cybersecurity best practices.

Future scope includes expanding the system with a mobile app, AI-driven crime pattern detection, chatbot support, and blockchain-based evidence verification.

# 2 Overall Description

## 2.1 Product Perspective

CIMAS is a replacement for fragmented, manual processes of reporting and investigating cybercrimes. By centralizing operations, it improves transparency, efficiency, and trust. It is an independent web-based system built using modern technologies for scalability and security.

## 2.2 User Classes and Characteristics

The system supports multiple user classes:

- **Victims / General Public** – Report incidents, upload evidence, view awareness content.
- **Investigators** – Access case details, update status, assign tasks, analyze evidence.
- **Administrators** – Manage users, oversee investigations, generate reports.
- **Awareness Hub Visitors** – Learn about safe online practices.

## 2.3 Product Functions

Core functionalities of CIMAS include:

- Incident reporting with secure evidence submission.
- Case assignment and progress tracking for investigators.
- Role-based access control to ensure secure operations.
- Crime mapping with location-based analytics.
- Awareness Hub containing guides, alerts, and best practices.

## 2.4 Operating Environment

- **Frontend:** React, JavaScript.
- **Backend:** Django Framework with PostgreSQL.

- **Supported OS:** Cross-platform (Windows, Linux, macOS).
- **Supported Browsers:** Chrome, Firefox, Edge, Safari.

## 2.5 Design

The system design includes:

- **Victim Workflow:** Register/login → Report incident → Upload evidence → Track case status.
- **Investigator Workflow:** Receive assigned cases → Review evidence → Update status/progress.
- **Administrator Workflow:** Manage users, oversee investigations, publish reports.
- **Awareness Hub:** Accessible without login, contains curated cybersecurity content.

# 3 System Features

## 3.1 Description and Priority

Priority features (highest to lowest):

1. Incident Reporting & Evidence Submission.
2. Case Management & Investigator Assignment.
3. Case Tracking & Notifications.
4. Crime Mapping & Analytics.
5. Awareness Hub.

## 3.2 Functional Requirements

- **Incident Reporting:** Victims can submit detailed complaints with attachments (images, documents, etc.).
- **Evidence Handling:** Secure storage with restricted access.
- **Case Assignment:** Administrators assign cases to investigators.
- **Progress Tracking:** Investigators update status; victims get notified.
- **Awareness Content:** Public access to safety guides, news, and alerts.

# 4 Other Nonfunctional Requirements

## 4.1 Performance Requirements

- The system should support multiple concurrent users with minimal latency.
- Database queries should return within 2 seconds under normal load.

## 4.2 Security Requirements

- Password hashing and secure authentication.
- Role-based access control (RBAC).
- Encrypted evidence storage and safe file handling.
- Regular audits for data protection compliance.

## 4.3 Software Quality Attributes

- **Usability:** Simple UI for victims and investigators.
- **Reliability:** Secure evidence storage and consistent system availability.
- **Scalability:** Capable of handling growing case reports.
- **Maintainability:** Modular architecture for easy upgrades.

## 4.4 Business Rules

- Only registered users can file incidents.
- Evidence can be accessed only by authorized investigators.
- Administrators approve investigator roles and oversee sensitive operations.

# 5 Other Requirements

- Mobile app development in future versions.
- AI-based crime pattern detection for predictive analysis.
- Chatbot support for faster complaint filing.
- Blockchain-based evidence verification to ensure integrity.