OROMIA POLICE COLLEGE

TITLE: CRIME RECORD MANAGEMENT SYSTEM FOR OROMIA POLICE COMMISION

Team Member

1. Ayele Nigusie
2. Yonas Gido
3. Kelbesa Merga

Adama, Ethiopia

Sept, 2025

Abstract

The Oromia Crime Record Management System (CRMS) is a web-based platform designed to streamline the recording, storage, and reporting of crime-related data in the Oromia region. The system provides law enforcement agencies with an efficient and secure way to manage crime record, generate reports, and enhance public safety. The system architecture is built using modern web technologies, ensuring scalability, security, and ease of access. This document provides a comprehensive overview of the system's objectives, features, architecture, database design, and workflow, alongside future enhancement possibilities such as AI-based crime pattern analysis and integration with national security databases.

Crime Record Management System (CRMS) – Functional and Non-Functional Requirements

1. Functional Requirements

1.1 User Management

- **User Creation & Role Assignment**
    - The system must allow administrators to create new users such as Admin, Officer, and Investigator**.**
    - A user creation form contains with the following fields:
        - Full Name
        - Email Address (required for account activation)
        - Phone Number
        - Birth date
        - Title
        - Role (Admin, Officer, Investigator.)
        - Organization Level (Region, Zone, Woreda, Kebele, Other)
        - Assigned Office/Location (linked to organization level, e.g., Woreda 05 Police Station)
        - Locale(Language choose)
        - Avator(Photo)
        - Education level
        - Biography
    - After registration, the system must:
        - Auto generate a temporary password.
        - Send an email notification with:
            - Username
            - Temporary password

- **Authentication & First Login Flow**
  - Users log in with the username and temporary password sent by email.
  - On first login, the system must enforce:
    - Changing the temporary password to a secure one.
    - Confirming the new password before gaining full access.
  - Until the password is changed, users cannot access any other feature.
- **Role-Based Access Control (RBAC) with Organization Levels**
  - The system must apply RBAC combined with organization hierarchy**.**
  - Access must be limited not only by role but also by organization level**:**
    - Regional Admin: Can manage and view all cases in their Region.
    - Zone Officer**:** Limited to Zone-level cases.
    - Woreda Officer: Limited to Woreda-level cases.
    - Kebele Officer: Limited to Kebele-level cases.
  - A role & level assignment form must allow admins to define both the user's role and their organization level**.**
- **User Profile Management**
  - Each user must have a profile page to update personal details.
  - Profile form fields:
    - Full Name
    - Gender
    - Email Address
    - Phone Number
    - Profile Picture (upload option)
    - Change Password (old password, new password, confirm new password)
    - Organization Level (view only, cannot change unless by admin)
- **Permission Management**
  - The system must allow administrators to add, edit, or delete permissions**.**
  - Permissions can be role-specific or level-specific (e.g., "View Cases at Region Level" vs "View Cases at Woreda Level").
- **Audit Trail & Activity Tracking**
  - The system must track user activities (e.g., login, logout, updates, and deletions).

- Logs must include timestamp, user ID, role, organization level, action performed, and affected records**.**
- Admins at higher levels (Region, Zone) can view logs of their sub-levels.

Crime Category and Sub-Category Management

The system must allow authorized users to create, read, and update daily statements. Daily statements record generic crime activity or occurrence without a certain accused or victim.

1. **Manage Categories**
   - Add a new crime category
     - Name
     - Code
     - Description
   - Edit/update existing categories.
   - Delete categories
   - View a list of all categories.
2. **Manage Sub-Categories**
   - Add subcategories under a specific category
     - Select Category
     - Name
     - Code
     - Description
   - Edit/update subcategories.
   - Delete subcategories (with data integrity checks).
   - View subcategories with their parent category.
3. **Validation & Access Control**
   - Only authorized users (Admin/Super Admin) can create, edit, or delete categories/subcategories.
   - Categories and subcategories must be unique.
   - When deleting, the system should prevent data loss by either blocking deletion or requiring reassignment of records.

4. **Integration**
    - Categories and subcategories must be selectable in:
        - Case/Crime Record Form
        - Daily Statement Form
        - Reporting & Analytics module

1.0 Daily Statement Management

The system must allow administrators to create and update crime categories and subcategories that may be used in case records, daily statements, and reports.

Features:

1.1. Create Daily Statement Form

The system shall provide a form with the following fields:

- **Statement Title/Name**
- **Category** (dropdown: Select Category)
- **Sub-Category** (dropdown: Select Sub-Category)
- **Description** (text area for incident details)
- **Date Reported** (calendar picker: mm/dd/yyyy)
- **Crime Happened At (Date & Time)** (datetime picker: mm/dd/yyyy --:-- --)
- **Region** (dropdown: Select Region)
- **Zone** (dropdown: Select Zone)
- **Woreda** (dropdown: Select Woreda)
- **Kebele** (dropdown: Select Kebele)
- **Specific Location** (text field)
- **X Axis (Latitude)** (decimal input)
- **Y Axis (Longitude)** (decimal input)

1.2 Crime Info-Eeruu Yakkaa

- **Crime/Case Registration**
  - The system must allow Police Officer to register new cases with structured details.
  - A case registration form must contains the following fields:
    - Case Number
    - Crime Category (dropdown: Crime against property, Crime against person, crime against state, etc.)
    - Crime Subcategory (dropdown based on selected category, e.g., Theft → Vehicle Theft, Pickpocketing, Housebreaking)
    - Case Description (detailed narrative of the incident)
    - Location Information**:**
      - Region (dropdown)
      - Zone (dropdown)
      - City
      - sub city
      - Woreda (dropdown)
      - Kebele (dropdown)
      - X-Axis (Longitude) – numeric field
      - Y-Axis (Latitude**)** – numeric field
    - Date and Time of Incident (date-time picker)
    - Manner of Submission(Haala Eerun Itti Dhiyaate) By person or mobile
    - Specific Location name
    - Compliant/ Victim Information (name, ID, contact, address, Education level , Ethnicity, Citizen sex , Age, Location sinature)
    - Suspect Information (name, ID, contact, address)
    - Manner of the Crime's Commission and Damage Caused
    - Eye Witness (full Name, Address)
    - Technical Witness
    - Investigator Full Name and signature
    - Attorney Full Name and signature
- **Case Search & Filtering**

- The system must provide advanced search and filtering by:
  - Case Number
  - Crime Category / Subcategory
  - Suspect Name
  - Victim Name
  - Case Type
  - Date / Time Range
  - Location (Region, Zone, Woreda, Kebele)
  - Coordinates (X, Y – for GIS-based search or map integration)
  - Case Status (Open, Under Investigation, Forwarded to Court, Closed)

- **Case Status Tracking**
  - Each case must include a status field with allowed states:
    - Open – newly registered.
    - Under Investigation – assigned and in progress.
    - Forwarded to Court – handed over to judiciary.
    - Closed – completed or resolved.
  - The system must record timestamps and remarks whenever status changes.
- **Investigator Assignment**
  - The system must support assigning cases to investigators across all organizational levels (Region, Zone, Woreda, Kebele).
  - Assignment functionality must include:
    - Assigning one or multiple investigators to a case.
    - Reassigning cases when necessary based on workload or organizational needs.
    - Sending immediate notifications (system alerts) to investigators whenever they are assigned or reassigned a case.
    - Tracking and displaying workload distribution to ensure balanced assignment across investigators.
- **Maintaining an assignment history log for accountability and auditing.Audit Trail**
  - Every case-related action must be logged, including creation, updates, reassignments, and closure.

  - Logs must capture:
    - Case ID
    - User ID
    - Role & Organization Level
    - Action Taken
    - Timestamp
    - Changed Fields (before & after values)

1.3. Investigation Management

- **Case Assignment to Investigators and Attorney**
  - The system must allow authorized users (e.g., Admins) to assign one or more investigators to a case.
  - Assignment must follow the organization hierarchy (Region, Zone, Woreda, Kebele).
  - Assigned investigators must receive notifications (system alert and/or email).
- **Progress Notes & Findings**
  - Investigators must be able to record progress notes and findings during an investigation.
  - A **progress note form** must include:
    - Date & Time of Entry
    - Investigator Name (auto-captured)
    - General attorney name
    - Case Reference Number

1.4. Accused, Victim, and Witness Management

- **Victim Information Recording**

The system shall allow investigator and attorney to record a victim's statement/testimony (Jechaa Himataa) and include an appointment date for follow-up. The system shall also generate a witness summons letter (xalayaa waamicha ragaa).

  - The system must allow entry of one or multiple victims per case.
  - A dedicated Victim Form must contain:
    - Full Name
    - Gender
    - Date of Birth / Age
    - National ID (if available)
    - Contact Information (phone, address)
    - Behavior
    - Appointment date
    - Print out witness Summons letter

- **Witness Information Recording on Appointment date (jecha Ragaa)**

The system shall allow officers to record witness statements on the scheduled appointment date, including eye witnesses, exhibit witnesses, and technical witnesses when available.

  - The system must allow linking of one or more witnesses to each case.
  - A Witness Form must contain:
    - Full Name
    - Gender
    - Date of Birth / Age
    - Contact Information (phone, address)
    - Witness Type (Eyewitness, Expert Witness, Character Witness, etc.)
    - Protection Required? (Yes/No toggle)

1.5. Suspect status

If the suspect's status is *arrested*, their information should be entered directly into the record. If the suspect is not arrested, they must be notified by a summons letter in accordance with Article 25, or be tracked by the police under Article 26.

This Form Must include:

- Reference Number
- Date and Time
- Full Name
- Police station Location
- Keyyata seera yakkaa either 25/26
- Sinear Director/commander sign

1.6. Suspect Property Record (Galmee Qabeenya Shakkamaa/Himatamaa)

The system shall allow users to record and track all items or exhibits related to a suspect or accused person. It shall capture item details, registration information, examination status, and the individuals associated with each item, ensuring proper documentation, verification, and full traceability.

This form must include:

- Serial No.
- Date Registered
- Number and Date Documented
- Sending Authority/Body
- Complainant/Plaintiff
- Accused/Suspect
- Exhibit Number
- Quantity
- Examination
- Examiner/Requester

1.7. Suspect Statement (Jecha Himatamaa)

The system shall allow officers to record the suspect’s statement (Jecha Himatamaa), including personal information, the suspect’s explanation of the incident, responses to allegations, and the date and time the statement is taken.

- The system must allow entry of one or multiple accused persons linked to each crime/case.
- A dedicated Accused Form must include:
    - Full Name
    - Gender
    - Date of Birth / Age
    - National ID / Passport Number (if available)
    - Contact Information (phone, address)
    - Photo (upload option)
    - Behavior

    - Progress Description / Findings
    - Related Person (Accused, Victim, Witness – linked via dropdown selection)
    - File Attachments (documents, images, videos, audio)

- **Multiple Entity Management**
    - Each case may contain:
        - Zero or more Accused.
        - One or more Victims.
        - One or more Witnesses.
    - The system must enforce data integrity by linking these entities to a single case record.
- **Search & Filtering**
    - The system must support searching and filtering by:
        - Accused Name
        - Victim Name
        - Witness Name

- National ID
- Case Number (to see all linked entities)

1.8. Bail Status Form (Haala Mirga Wabii / Unka Dirqama Wabii)

The system shall allow recording and management of bail obligations for suspects released under legal provisions. It shall capture guarantor information, details of the bail obligation, and compliance status, ensuring accountability and traceability for suspects released on bail.

This Form **must include:**

- Date
- Guarantor's Information
- full Name
- Town/City Address
- Kebele/Village
- Phone Number
- Sub-City
- House Number
- Job/Role
- Marital Status
- Obligation Statement

1.9.Investigation File Completion Letter (Xalayaa Galmee Qorannaa Xumurame Eerguu)

The system shall allow the creation and sending of letters for completed investigation files, indicating their status as **Closed**, **Proceed**, or **Reinvestigate**. It shall capture reference numbers, dates, suspect details, and a summary of all included documents with file and page numbers. The system shall ensure proper documentation, traceability, and confirmation of delivery to the receiving authority.

This Form **must include:**

- Case File Title
- Initial Complaint/Report

- Statement of the Accuser/Complainant
- Statement of the Suspect
- Statement of the Witness
- Results of Various Investigation Documents/Evidence
- Status Either Proceed, closed , reinvestigate

1.10. Crime Record Registration When Proceeding to Court

The system shall allow comprehensive registration and monitoring of crime cases that proceed to court. It shall capture detailed information about the crime, suspects, complainants, demographic and socio-economic data, location, investigations, judicial proceedings, and related files. The system shall ensure traceability, accountability, and support proper follow-up and reporting of criminal cases.

1.11.Final Investigation Report

- The investigators must be able to make a final investigation report, aggregating all activity related to it.
- The final report must include:
    - Case Reference Number
    - Name(s) of Investigator(s)
    - Summary of Progress Notes
    - Records of Interviews (related to accused, victim, witness details)
    - Inspection Reports & Evidence Findings
    - Key Conclusions and Recommendations
    - Decision (Forward to Court, Close Case, Reinvestigate)
    - File Attachments (forensic outputs, scanned reports, etc.)

1.12. Statements/Interviews Management

The system should allow administrators and approved officials to add, edit, and manage statements/interviews of accused, victims, and witnesses related to crime records.

- **Create Statements/Interviews Form**
    - The system shall include a form with the following fields:

        - Crime ID (dropdown: Select Crime Record)
        - Party Type (dropdown: Accused / Victim / Witness)
        - Party ID (dropdown: Select Party from respective list)
        - Statement/Interview Title (text field)
        - Statement/Interview Description (text area for detailed input)
        - Date & Time of Statement/Interview (datetime picker: mm/dd/yyyy --:-- --)
        - Officer/Interviewer Name (text field or dropdown referencing system users)
- **Manage Statements/Interviews**
    - The system must allow the following operations for statements/interviews by users:
    - Create, view, update, and delete statements/interviews.
    - The system must allow filtering and search for statements/interviews on:
        - Crime ID
        - Party Type (Accused, Victim, Witness)
        - Date of Interview
        - Display & Reports
- For each Crime Record, the system must display all associated statements/interviews grouped by:
    - Accused Statements/Interviews
    - Victim Statements/Interviews
    - Witness Statements/Interviews
- The system must enable the generation of a compiled report showing all statements/interviews related to a specified Crime ID.

1.13. Organization Structure Management

- **Organizational Hierarchy**
    - The system must allow the registration and management of the police organizational structure**.**
    - Levels to be supported include:

        - Region
        - Zone
        - Woreda
        - Kebele
        - Police Station / Sub-Station
    - The system must allow flexibility to add other levels if required.

1.14.Reporting & Analytics

- **Crime Statistics & Trends**
    - The system must be able to generate crime statistics and analytical reports.
    - Reports must allow filtering and grouping by:
        - Crime Type
        - Crime Subcategory
        - Location (Region, Zone, Woreda, Kebele, GPS coordinates)
        - Date & Time (daily, weekly, monthly, yearly trends)
        - Gender
    - The system should provide trend analysis (e.g., increase/decrease in specific crime types over time).
- **Case Status Reports**
    - The system must generate reports on case statuses**,** including:
        - Open Cases
        - Ongoing / Under Investigation
        - Forwarded to Court
        - Closed Cases
    - Reports must allow filtering by date range, investigator, or organizational level**.**
- **Dashboards & Visual Analytics**
    - The system must display interactive dashboards with graphical overviews for quick decision-making.
    - Dashboards must include:
        - Charts & Graphs (crime trends by type, location, time)
        - Tables (detailed case lists, user activities, investigation summaries)

    - Dashboards must support real-time updates and allow data export (PDF, Excel).
- **Export & Sharing**
    - All reports must be exportable to PDF, Excel, and CSV**.**
    - Reports must be shareable with authorized users only, respecting access control rules

.2 .Non-Functional Requirements

2.1 Performance

- ✓ The system must support at least 200 concurrent users.
- ✓ The system dashboards and records must load within 3 seconds on standard network connections.
- ✓ The system must allow upload and storage of files up to 100MB.

2.2 Usability

- ✓ The system must provide a simple, user-friendly interface for all users.
- ✓ The system must be available in English and Afan Oromo version.
- ✓ The system must be accessible via different platform like desktop and mobile devices.
- ✓ The system must provide help tips and guidelines for common tasks.

2.3 Reliability & Availability

- ✓ The system must ensure 99% uptime during working hours.
- ✓ The system must automatically back up data daily.
- ✓ The system must support redundant servers to avoid downtime.

2.4 Security

- ✓ The system must encrypt all user passwords.
- ✓ The system must enforce secure communication via HTTPS/SSL.
- ✓ The system must lock accounts after multiple failed login attempts.
- ✓ The system must log all create, update, and delete actions.

2.5 Data Integrity

- ✓ The system must validate all inputs before saving to the database.
- ✓ The system must not allow duplication of case numbers.
- ✓ The system's critical records must not be deleted without administrator approval.

2.6 Scalability

- ✓ The system must support integration with additional police stations.
- ✓ The system must handle growth in crime records without performance issues.
- ✓ The system must allow integration with future national police databases.

2.7 Maintainability

- ✓ The system must use modular architecture for easy upgrades.
- ✓ The system must maintain error and activity logs for troubleshooting.
- ✓ The system must allow software updates without affecting existing data.

2.8 Legal & Compliance

- ✓ The system shall comply with Ethiopian data protection regulations.
- ✓ All data shall be kept confidential and accessed only by authorized users.
- ✓ Reports generated shall meet legal standards for court submission.

2.9 User Support, Documentation & Training

- ✓ A User Manual shall be prepared, covering system features, workflows, troubleshooting steps, and security guidelines.
- ✓ An Administrator Guide shall be provided for system configuration, role management, and maintenance procedures.
- ✓ The system provider shall deliver user training sessions (onsite or virtual) for:
    - o Investigators
    - o Police officers
    - o Administrators

- ✓ Training materials (slides, quick reference guides) shall be included for future onboarding.
- ✓ The system shall include contextual help or tooltips to assist users during operation.
- ✓ Updates to the manual and training materials must be provided with every major system upgrade.