

# PROJECT PROPOSAL

## Integrated Vigilance Case Management & Digitization Platform

### 1. Background & Objectives

---

VACB currently processes complaints, enquiries and cases through a combination of manual registers, disparate spreadsheets and limited point solutions. This fragmentation results in duplicate data entry, delayed reporting, and limited visibility into case status and officer workload across districts and units.

The proposed platform aims to digitize the complete case-processing lifecycle — from petition intake through investigation, prosecution and court disposal — on a single, secure, government-hosted system, while introducing AI-assisted analytics to support proactive vigilance.

#### Key Objectives

- Provide a single point of intake for complaints from web, mobile app, WhatsApp, email, toll-free number, physical submission, district units and social media.
- Digitize the full case lifecycle — Confidential Verification (CV), Quick Verification (QV), Preliminary Enquiry (PE), Vigilance Enquiry (VE), Surprise Check (SC) and Vigilance Case (VC) — with defined approval hierarchies.
- Eliminate duplicate data entry across the Petition → FIR → Case Management → Court workflow through automatic data flow between modules.
- Introduce AI-assisted analytics for complaint classification, risk scoring, anomaly detection and corruption hotspot identification.
- Improve transparency, traceability and management oversight through dashboards, MIS reporting and a centralised document repository.

### 2. Functional Scope of Work

---

The platform to be implemented shall comprise the following thirteen (13) functional modules. Detailed requirements for each module are set out below; bidders shall propose their technical approach against each of these requirements in their technical proposal.

#### 2.1 Citizen Centric Complaint Management System (C3MS)

- Unified intake of complaints from website portal, mobile app, WhatsApp, email, toll-free number/call centre (IVR), physical/walk-in submission, district units and social media leads, into a single petition database.
- Auto-generation of a unique petition/token number on submission through any channel, with acknowledgement sent to the complainant via SMS/email/WhatsApp where contact details are available.
- Structured petition form capturing complainant details, an option for confidential/whistle-blower submission, nature of complaint, department/officer(s) involved, and upload of supporting documents/evidence.

- Automated duplicate and repeat-complaint detection against the existing petition database.
- Rule-based routing/assignment of petitions to the appropriate unit or officer based on jurisdiction, department and category.
- Complainant-facing status tracking (where disclosure is appropriate) and internal officer dashboard of petitions by stage and ageing.
- SLA-based reminders and escalation for petitions pending beyond defined timelines, and seamless handoff into the Complaint Categorization Framework and Vigilance Case & Enquiry Management System (VCEMS).

## 2.2 Complaint Categorization Framework

- Admin-configurable master list of complaint categories, corruption-types and applicable statutory provisions.
- AI-assisted auto-tagging/classification of incoming petitions using NLP on the complaint narrative and digitized supporting documents.
- Officer-driven manual review and re-categorization, with a full audit trail of any change to the AI-assigned category.
- Multi-level categorization (primary category, sub-category, relevant section of law) to support both case routing and statutory/statistical reporting.
- Category-based routing rules — for example, automatically flagging certain categories for direct Confidential Verification (CV) or Quick Verification (QV) rather than a routine Preliminary Enquiry (PE).
- Category-wise trend reporting, feeding into the AI Analytics Engine and heat-map/predictive-vigilance visualisation.

## 2.3 Vigilance Clearance & NOC Management

- Digital application form for vigilance clearance/NOC requests (e.g. promotion, deputation, foreign travel, empanelment) from departments or individuals.
- Automated cross-check of the applicant against the case/complaint database to flag any pending or past vigilance action, surfaced to the approving officer before clearance is granted.
- Configurable, hierarchical approval workflow up to Director level, with the approval chain adjustable by clearance type.
- SLA tracking and escalation for pending clearance requests, with status visibility to the requesting department.
- Digitally signed clearance/NOC certificate generation bearing a unique reference number and verification mechanism (e.g. QR code).
- Searchable repository of all issued clearances, for future reference, audit and RTI response purposes.

## 2.4 Internal Vigilance Cell Management

- Central repository for information shared by Internal Vigilance Cells (IVCs) of individual government departments across the state.

- Structured intake of IVC referrals and reports, automatically cross-linked to VACB's central case database to avoid duplicate or parallel proceedings.
- Role-based access so that each IVC can view and manage only its own department's submissions, while VACB retains statewide visibility.
- Workflow enabling VACB to review, comment on, and where required take over or advise on cases raised by an IVC.
- Consolidated, statewide dashboard of IVC activity, case status and department-wise vigilance trends.
- Secure, auditable document exchange between IVCs and VACB.

## 2.5 Open Source Intelligence (OSINT)

- Automated monitoring of configured news portals, public websites and social media sources for corruption-related mentions of officers, departments or entities.
- Configurable keyword and entity watchlists, with alerts routed to designated intelligence officers.
- AI-assisted relevance scoring and de-duplication/noise-filtering of captured leads before they reach an officer's queue.
- Workflow to convert a validated OSINT lead into a formal petition or Confidential Verification (CV) within VCEMS, preserving the source and capture-time record.
- Automatic tagging of captured leads against the relevant officer/entity dossier in the Dossier & Intelligence repository.
- Full audit trail (source, capture timestamp, reviewing officer) for every OSINT item, to preserve evidentiary integrity.

## 2.6 AI Analytics Engine

- NLP-based text analytics on petitions, enquiry reports and Case Diary entries for classification, summarisation and entity extraction.
- A risk-scoring model combining complaint frequency, category severity, officer history and OSINT signals to flag high-risk cases or individuals for review.
- Anomaly detection across available departmental data feeds to flag irregular patterns warranting a Preliminary Enquiry.
- Predictive analytics for case-load forecasting and resource/officer-deployment planning.
- Configurable model thresholds with an explainability layer (reason codes) so that every flagged item is reviewed and validated by an officer rather than acted upon automatically.
- Officer feedback loop to mark false positives, so model accuracy improves over time.
- GIS-based heat maps for corruption hotspot identification and departmental risk analysis, built on the same analytics layer.

## 2.7 Officer Performance Management

- Officer-wise workload dashboard showing assigned petitions/cases/enquiries by stage, category and ageing.

- Automated workload-balancing suggestions at the point of assigning a new petition or case.
- Competency scoring based on case disposal timelines, quality indicators (e.g. cases upheld versus returned for review) and training completion.
- Performance dashboards at officer, unit and district level for supervisory review.
- Configurable KPIs with periodic (monthly/quarterly) performance reports for management.

## **2.8 Training & Capacity Building**

- Training-needs identification linked to skill-gaps surfaced from the Officer Performance Management module.
- Digital nomination workflow for officers to be enrolled in training programmes, with approval routing.
- Certification tracking — record of trainings completed, certificates issued, and validity/renewal dates.
- A training calendar and a resource repository (materials, SOPs, case studies) accessible to officers.
- Reporting on training coverage across units, to support statewide capacity-building planning.

## **2.9 Asset & Inventory Management**

- Digital register of departmental assets — vehicles, IT equipment, office equipment, surveillance/forensic equipment — each with a unique asset ID.
- Allocation and custody tracking of assets to units/officers, with a full assignment history.
- Maintenance scheduling and service-history logging for critical assets.
- Procurement-request workflow with approval routing.
- Depreciation/write-off tracking, and support for periodic physical-verification reconciliation.
- Asset-utilisation and inventory-level reporting.

## **2.10 Legal & Prosecution Management**

- Digital tracking of court cases linked to each Vigilance Case (VC), including case number, court, hearing dates and current status.
- Sanction-for-prosecution request and approval workflow, with a document repository for sanction orders.
- Appeals and revision tracking, linked to the originating case.
- Hearing-date calendar with automated reminders to the concerned Investigating/Prosecuting Officer and Public Prosecutor.
- Digital repository of charge sheets, evidence lists and legal correspondence, linked to the Case Diary.
- MIS reporting on prosecution pendency, conviction rates and case ageing for legal review.

## **2.11 Dashboard & Command Centre**

- Executive dashboard providing a real-time, statewide overview of complaint volumes, case-status distribution, and unit-wise pendency and ageing.
- Drill-down capability from the statewide view to district, unit, officer and individual-case level.

- A command-centre view combining case data with OSINT alerts and heat-map/GIS visualisation for situational awareness.
- Role-based dashboard views (Director, unit heads, officers) surfacing only the data relevant to that role.
- Configurable widgets/KPIs, with exportable summary reports for leadership briefings.

## 2.12 Reporting & MIS

- Standard and ad-hoc report generation across all modules — petitions, cases, clearances, prosecution, training and assets.
- Operational reports (daily/weekly pendency, SLA breaches), tactical reports (unit/category trend analysis) and strategic reports (annual statistics and statutory reporting formats) as required by VACB and Government of Kerala.
- Export in standard formats (PDF/Excel) with support for scheduled, automated report delivery to designated recipients.
- Audit-log reporting to support compliance review and internal oversight.

## 2.13 Mobile Application

- A citizen-facing mobile app (Android and iOS) for complaint filing, status tracking and secure two-way communication on case status, subject to applicable disclosure rules.
- An officer-facing mobile app for field operations — case updates, document capture (photo/scan upload), digital completion of Mahazar/inspection-memo forms, and offline-capable data entry that syncs once connectivity is restored.
- Push notifications/alerts for citizens (status updates) and officers (task assignments, SLA reminders).
- Secure, OTP-based authentication with role-based access mirroring the web platform.
- Location capture during field visits/surprise checks, feeding into the GIS-based heat maps in the AI Analytics Engine.

## 3. End-to-End Case Processing Digitization (Petition → FIR → VCEMS → Court)

---

The platform shall provide automated, checklist-driven digitization of the full case-processing lifecycle, eliminating duplicate data entry between modules and digitizing all case-related documentation.

### Petition-to-FIR Automation

- On petition finalization, relevant petition data shall flow automatically into the FIR Information section, with no manual re-entry.
- FIR Information shall be sourced directly from the Petition Module; officers review and proceed with the FIR process rather than editing data manually.
- Once the FIR process is completed, FIR-related data shall automatically flow into the FIR Module.

### FIR & VCEMS Integration

- The VCEMS section shall be integrated with the FIR Module.
- On completion of the FIR section, the first section of the Case Diary shall be automatically created, using FIR information as the foundation for subsequent case processing.
- The integrated workflow shall reduce duplicate data entry and improve cross-module consistency.

#### **Case Diary & Document Management**

- A centralized Case Diary shall maintain all documents and information associated with a case, with each document assigned a unique Document ID/Number.
- Document metadata captured shall include Document ID/Number, number of pages, date and case-related document details.
- Every document and case-related item shall be assigned a unique number for identification and tracking.
- The Informational Report shall form the initial digitization stage, with report data converted to a structured, searchable digital format linked to the respective case.

#### **Standardized Document Templates**

- Predefined, authorized templates shall be provided for major case-related documents, selectable by officers during case processing, including Warrant, Mahazar, Case Property/Exhibit, Inspection Memo, Arrest Request and other required templates.
- Standardized templates shall reduce manual document preparation and ensure uniformity across cases.

#### **Arrest Processing & Arrest Information Module**

- A Digital Arrest Memo shall allow officers to select the relevant Case Diary and Warrant, then complete and submit the Arrest Memo form digitally for officer verification.
- A dedicated Arrest Information Module shall manage arrest-related information, with scan-and-upload of documents and auto-assigned unique document numbers, all linked to the respective case.
- Provision shall be included for uploading medical reports as part of arrest documentation.

#### **Case File Search, Retrieval, Search & Download**

- Filter-based search across multiple criteria for fast, targeted retrieval of case files.
- Single-file download and bulk download of multiple files simultaneously, through a centralized, unified interface.

#### **Complete Digitization & Modernization**

- End-to-end digitization of the complete case management workflow, reducing dependency on physical documentation.
- Digital signature capability for authenticated digital execution of case documents.
- Digital submission of case records to court, with improved visibility, traceability and accessibility of records across the workflow.

#### **Activity-Based Checklists & Progress Monitoring**

- Each major activity shall have a predefined set of sub-activities and a dedicated checklist, so officers can clearly identify what must be completed before closing an activity.
- Checklist completion shall be used to track activity status, sub-activity completion, pending and completed activities, and overall case progress.
- Reports generated from activity/checklist completion shall support monitoring, review and management-level reporting.

#### **Key Benefits**

- Automatic data flow across Petition → FIR → VCEMS, eliminating duplicate data entry.
- Standardized case documentation through authorized templates, with complete digital document management, unique numbering and traceability.
- Digital arrest processing and centralized Case Diary management.
- Advanced search with single-file and bulk download capabilities.
- Digital signatures and digital court submission.
- Checklist-based activity monitoring for improved case tracking and transparency.

## 4. Technical & Platform Scope

---

- Enterprise Architecture: multi-layer architecture spanning citizen/officer channels, application layer, integration layer, analytics layer, AI layer and security layer.
- Integration Framework: API gateway-based integration with existing systems — DSMS, iAPS, eOffice and other external/departmental systems.
- Data Architecture: master data management, metadata standards and enterprise data governance.
- Privacy & Compliance: compliance with applicable government data policies, audit requirements and records-retention schedules.
- Infrastructure Architecture: cloud and/or on-premises deployment options, disaster recovery (DR) site and business continuity planning.
- Mobile Applications: dedicated mobile interfaces for citizens (complaint filing/tracking) and for VACB officers (field operations).
- Dashboard & Command Centre: executive monitoring dashboards and an operational command-centre view.
- Reporting & MIS: operational, tactical and strategic reporting across all modules.

AI-assisted capabilities — including document reading/classification, voice transcription and multi-language content translation — shall be scoped and costed by the implementing partner as part of the commercial proposal, based on projected transaction volumes to be shared during the tender process.

## 5. Implementation Scope

---

- Project Governance: establishment of a steering committee, PMO structure and implementation oversight mechanism, with VACB and the implementation partner represented.
- Implementation Methodology: a phased implementation approach is envisaged.
- Indicative Phase-wise Rollout: Phase 1 – core modules; Phase 2 – system integrations; Phase 3 – AI and analytics capabilities. Bidders shall propose a detailed implementation timeline as part of their technical proposal.
- Change Management: a user-adoption plan and organizational transformation strategy shall be developed jointly with VACB.
- Training Plan: a structured rollout and user-enablement programme for VACB personnel across all units.
- Post-implementation support: the selected partner shall be required to propose warranty/bug-fix support and an Annual Maintenance Contract (AMC) structure as part of the commercial proposal.

## 6. Commercial Terms

---

This proposal is submitted for the purpose of seeking Kerala Startup Mission's facilitation in identifying a suitable implementation partner, and does not itself constitute a commercial offer. No pricing or cost figures have been included in this document.

Organisations shortlisted or empanelled through the process facilitated by Kerala Startup Mission shall be required to submit detailed, itemised pricing — covering software development, AI/analytics implementation, mobile applications, third-party integrations (e.g. messaging/OTP services) and Annual Maintenance Charges — in a separate commercial proposal sheet, in the format to be prescribed at the tendering stage. Applicable taxes (GST) shall be indicated separately by each bidder.

## 7. General Terms & Conditions

---

- This proposal, and the process it initiates, shall be governed by the applicable Government of Kerala procurement rules and Kerala Startup Mission's empanelment/facilitation guidelines.
- Technical and commercial proposals from participating organisations shall be evaluated separately, in line with the standard two-envelope tender methodology.
- The selected implementation partner shall be required to comply with applicable government data security, hosting and audit requirements, including a mandatory Vulnerability Assessment & Penetration Testing (VAPT) of the deployed system prior to go-live.
- VACB reserves the right to seek clarifications, request proof-of-concept demonstrations, or modify the scope of this proposal at any stage of the facilitation process.

— End of Proposal —