Annexure 1

Request for Proposal (RFP) for Financial Fraud Complaint Tracking System (FFCTS).

Introduction:

The Police Department invites proposals from qualified vendors to implement a Complaint Tracking System tailored for addressing financial fraud. The primary objective is to streamline the reporting and handling of financial fraud complaints, fostering a secure environment and strengthening our response to white-collar crimes effectively.

Project Overview:

The Financial Fraud Complaint Tracking System should be a comprehensive solution, incorporating advanced features for seamless case tracking, and robust data analysis. The goal is to enhance our capability to combat financial crimes through a modern, user-friendly, and technologically advanced system. Interested vendors are invited to submit proposals aligned with these objectives. The selected firm will be responsible for conducting an in-depth system study, analysing existing processes, and identifying areas for improvement. The findings will be crucial in guiding the development of a customized software solution that aligns with the department's goals and enhances operational efficiency.

Scope of Work:

1. Evaluate existing systems, processes, and workflows.
    - Identify current challenges, bottlenecks, and areas for improvement.
    - Assess user requirements and expectations.
    - Provide recommendations for optimizing processes through software implementation.
2. User-Friendly Interface:
    - An intuitive platform for to submit financial fraud complaints easily.
3. Complaint Intake:
    - The system should allow for the intake of financial fraud complaints in a variety of formats.
    - User-friendly and comprehensive data entry module specifically tailored for financial fraud complaints.
    - The system should allow for the import of financial fraud data from Excel spread sheets and the export of data to Excel spread sheets.
    - Facility to export excel sheet with the following fields

Data Fields

1. "Sl. No"
2. Date of entry
3. Time of Entry

4. Acknowledgement No.
5. District
6. Victim Bank
7. Amount lost from victim account
8. Transaction date & time
9. Amount on Hold
10. HOLD BANK
11. Amount lost from ecosystem
12. Date of such withdrawal
13. Time of Withdrawal
14. "W/D Bank Details"
15. Amount for pending action
16. Action Pending with
17. Assigned to
18. Reason for pendency
19. Modus operandi

4. User Management:
   - Interface for creating, modifying, and deactivating user accounts.
   - Role-based access control to manage permissions.
   - Configurable reporting structures to reflect our organization's hierarchy.
   - Ability to visualize and modify reporting relationships.
   - Role-based permissions to ensure security and compliance.
   - Ability to scale up as our system grows, accommodating an increasing number of users and reporting structures.
   - Logging of user activities and changes made to user profiles.
   - Provision to manually assign cases to users on a day-by-day basis for further processing.
5. Complaint Tracking:
   - A robust tracking system to monitor the progress of complaints from submission to resolution.
6. Multi-Department Collaboration:
   - Facilitate collaboration among various departments involved in investigating financial fraud cases.
7. Data Security:
   - Implementation of advanced security measures to safeguard sensitive information related to financial fraud cases.
8. Reporting Module
   - The reporting module should generate comprehensive reports on financial fraud trends, patterns, and statistics. These reports will be used to identify emerging trends, inform investigative strategies, and allocate resources effectively. The reporting module will allow users to:
     1. Generate reports on the volume, type, and severity of financial fraud complaints.
     2. Analyse geographical trends and identify areas with high concentrations of fraud.
     3. Track the success of investigative efforts and identify areas for improvement.

4. Generate reports on specific fraud schemes and identify common modus operandi.

- Money Loss Timing Analysis: This report should compare the time of withdrawal with the date and time of the report to determine whether the money was lost before or after the case was reported.
- Suspect Account Notices: This report should generate individual or bulk notices for each suspect account, notifying the relevant banks of potential fraud activity.
- Bank Response Time Visualizations: This report should incorporate diagrams and charts to visually represent the response times of different banks in handling financial fraud cases.
- Data Percentage Analysis: This report should calculate the percentage of data related to the amount on hold, lost, and pending for action.
- Total Count of Cases: This report should provide a summary of the total number of financial fraud cases handled by the organization, excluding reassigned and wrong cases.
- Total Amount Reported: This report should calculate the total amount of money reported as lost due to financial fraud, excluding reassigned data.
- Total Amount on Hold: This report should identify and quantify the total amount of money currently on hold due to financial fraud investigations.
- Total Amount Lost from the Ecosystem: This report should determine the total amount of money permanently lost due to financial fraud.
- Total Amount Pending for Action: This report should identify and quantify the total amount of money pending action from banks, along with the specific bank responsible for each case.
- Bank Response Time: This report should analyze the response time of banks in handling financial fraud cases by comparing the reported date and time to the time of action taken by each bank.
- Modus of Each Case: This report should categorize financial fraud cases based on their modus operandi, providing insights into the most common types of fraud.
- Suspect Account Identification: This report should automatically identify and list the account numbers of suspects involved in financial fraud cases, excluding the victim's accounts.
- Money Loss Timing Analysis: This report should compare the time of withdrawal with the date and time of the report to

determine whether the money was lost before or after the case was reported.

- Suspect Account Notices: This report should generate individual or bulk notices for each suspect account, notifying the relevant banks of potential fraud activity.
- Bank Response Time Visualizations: This report should incorporate diagrams and charts to visually represent the response times of different banks in handling financial fraud cases.
- Data Percentage Analysis: This report should calculate the percentage of data related to the amount on hold, lost, and pending for action.
- Data Consolidation: The software should allow users to consolidate data from the above reports individually or in bulk, with options to generate reports in Excel, PDF, or CSV formats.
- Automated Report Generation: The software should enable automated report generation, including the sending of Excel files via email.
- Withdrawal Case Identification: The software should identify withdrawal cases and provide details such as account number, time of withdrawal, and amount withdrawn.
- Cases above 1 Lakh Report: This report should identify and generate a separate report for financial fraud cases involving amounts greater than 1 lakh.

9. User Level Management Module
   - The user level management module will control access to the FFCTS based on user roles and permissions. This will ensure that only authorized personnel have access to sensitive case information. User roles will include:
   - Investigators: Full access to all case information and functionalities.
   - Supervisors: Limited access to case information, with the ability to review and approve investigative actions.
   - Administrators: Full administrative control over the system, including user management and system configurations.
   - The user level management module should also provide an audit trail to track all user activity within the system, ensuring accountability and preventing unauthorized access or modifications to case information.

8. Officer Access and Reporting:
   - Ensure various reports are accessible to higher officers for better decision-making.
9. NCRP Integration: The system should include a provision for future integration with the NCRP to enable seamless data sharing between the two systems.

Submission Requirements:

Interested web application development start-ups are requested to submit the following:

1. **Company Profile:**
   - Overview of your company's experience and expertise in web application development.
2. **Portfolio:**
   - Examples of similar web application development projects you have completed.
3. **Technical Proposal:**
   - Detailed technical approach for upgrading the website.
4. **Timeline:**
   - Project timeline with milestones and deadlines.
5. **References:**
   - Contact information for at least three client references for whom you have completed similar projects.

Evaluation Criteria:

Proposals will be evaluated based on the criteria established by Start-up Mission and the following:

a) Experience and expertise in development and website based applications.

b) Technical approach and methodology.

c) Cost-effectiveness.

d) Compliance with government guidelines.

e) Timeliness and project management capabilities.

f) Additional services recommended by the firm to enhance the functionality and security of the website.

1. Timeline:

a) RFP Issuance Date: 21/11/2023

b) Proposal Submission Deadline: 05/12/2023

c) Evaluation and Selection: 05/12/2023 to 08/12/2023

d) Project Commencement: 15/12/2023

2. Contact Information:

For any inquiries or clarifications regarding this RFP, please contact to Mr. Abdul Rassi .A (9895258496 / 9497936102 / 8893567830) or Email: "webadminscrb.pol@kerala.gov.in".

Kerala Police looks forward to partnering with an experienced and innovative web application development company. We appreciate your interest and efforts in responding to this RFP.

****