Requirement Document: Police Brutality Reporting System

1. Introduction

1.1 Project Overview

The Police Brutality Reporting System is designed to allow Nigerian citizens to report incidents of police misconduct and brutality. The platform ensures secure, evidence-backed reporting using National Identification Number (NIN) for authentication.

User data and identities will be encrypted to protect privacy. Reports are geo-tagged and automatically routed to the nearest police station, with escalation mechanisms in place for unresolved cases.

2. Objectives

* Empower citizens to report police brutality safely and securely.
* Ensure evidence-backed reporting to minimize false claims.
* Route reports to the nearest police station automatically.
* Escalate unresolved reports to higher authorities.
* Provide transparent case tracking for users.
* Protect users identities with encryption and anonymization.

3. Scope

* User Categories: Citizens, Moderators, Admins.
* Platforms: Web, Mobile (Android/iOS).
* Regions Covered: Nationwide with localized reporting.
* Data Handling: Secure, encrypted storage and transfer.
* Incident Categories: Physical assault, extortion, harassment, illegal detention, etc.

4. System Features

4.1 User Authentication and Security

* NIN and password-based login.
* Two-factor authentication (2FA).
* Data encryption (AES for storage, RSA for sensitive information).
* Role-based access control (RBAC).
* Rate Limiting to Prevent System Abuse:
  + Implement IP-based rate limiting: Maximum of 3-5 reports per hour from the same IP.
  + Add CAPTCHA verification for multiple rapid submissions.
  + Create a scoring system for reports based on evidence quality and user history.
  + Add automatic flagging for suspicious patterns (e.g., multiple similar reports in short timeframes).

4.2 Reporting Features

* Incident type selection (dropdown with categories).
* Region and area selection (Google Maps API integration).
* Evidence uploads (photos, videos, audio files).
* Anonymous reporting option.
* Live streaming for real-time incident capture.
* Automatic timestamping.
* Anonymous Reporting Protection:
  + Generate random, single-use report identifiers with no connection to user data.
  + Strip metadata from uploaded media files automatically.
  + Use Tor-like routing for report submission to mask IP addresses.
  + Implement zero-knowledge proofs for NIN verification without storing identity.
  + Create separate database partitions for identity data and report content.
  + Add options for delayed report submission (to prevent time correlation).

4.3 Report Management

* Unique tracking ID for each report.
* Report status tracking (Received, In-progress, Escalated, Closed).
* Automated email routing to the nearest police station.
* Escalation to higher authorities if no action within 7 days.
* Whistleblower Protection Measures:
  + Implement secure dead-man's switch protocols (automated evidence release if user doesn't check in).
  + Create emergency legal aid hotline integration.
  + Add automatic notification system to trusted NGOs when high-risk reports are filed.
  + Implement secure document vault for sensitive evidence with multi-party access control.
  + Create witness collaboration tools with end-to-end encryption.
  + Add option for automatic report duplication to multiple oversight bodies.

4.4 Notification System

* SMS and email confirmation on report submission.
* Push notifications for status updates.
* Reminder notifications for unresolved cases.

4.5 Dashboard and Analytics

* Public-facing dashboard with anonymized data.
* Admin dashboard with detailed incident reports.
* Aggregated reports by region, category, and resolution status.

4.6 Secure Evidence Handling

* Implement blockchain-based evidence timestamping.
* Create unalterable audit logs for every access to evidence.
* Add automatic video/image authenticity verification.
* Implement digital signatures for all uploaded evidence.
* Create clear chain of custody documentation with role-based access logs.
* Add automatic backup to multiple secure locations.
* Implement evidence classification system based on sensitivity.

5. Technical Requirements

5.1 Frontend

* Framework: React (Web), Flutter (Mobile).
* Language: JavaScript, Dart.
* Design: Responsive and accessible UI/UX.
* API Integration: Google Maps API for location services.

5.2 Backend

* Framework: ASP.NET Core.
* Database: MySQL.
* Authentication: NIN API integration.
* Encryption: AES (256-bit) for data storage, RSA for sensitive data.
* Email Service: SendGrid or SMTP.

5.3 Infrastructure

* Cloud Hosting: AWS or Azure.
* Load Balancing: Horizontal scaling for traffic management.
* Backup: Automated data backup every 24 hours.

6. Workflow

User Sign-in:

* User enters NIN and password.
* 2FA is prompted.
* System validates credentials through NIN API.

Submit Report:

* User selects incident type.
* Provides incident description, selects location.
* Uploads evidence.
* Option to report anonymously.

Routing:

* Report is geo-tagged and sent to the nearest police station.
* User receives email/SMS confirmation with tracking ID.

Tracking and Escalation:

* User tracks report status via dashboard.
* If no action within 7 days, the report is escalated to higher authorities.

7. Service Level Agreements (SLAs)

* Critical Incidents (Violence, Life-threatening): 1-hour response, 24-hour investigation initiation.
  + Serious Misconduct: 4-hour response, 48-hour investigation initiation.
  + General Complaints: 24-hour response, 72-hour investigation initiation.
  + Automatic escalation triggers when SLAs are breached.
  + Real-time SLA monitoring dashboard.

8. Escalation Paths

* Level 1: Local Police Station Commander.
* Level 2: State Police Commissioner.
* Level 3: Police Service Commission.
* Level 4: National Human Rights Commission.
* Level 5: Federal Ministry of Justice.
* Parallel escalation to:
  + Independent Police Oversight Bodies.
  + Public Complaints Commission.
  + Relevant Legislative Committees.
  + Automatic notification to media oversight committees for critical cases.

9. Potential Risks and Mitigation

* Security Breach:
  + Mitigation: Data encryption, periodic penetration testing.
* False Reports:
  + Mitigation: Evidence submission required, penalty for fake reports.
* Police non-response:
  + Mitigation: Automatic escalation, third-party monitoring (NGOs).

10. Additional Features (Future Scope)

* Blockchain integration for immutable evidence storage.
* AI-based evidence analysis.
* Offline SMS-based reporting.
* Reward mechanism for verified reports.
* Integration with civil rights groups.
* Implement end-to-end encrypted messaging system.
* Add secure video conferencing capability for remote interviews.
* Create anonymous tip submission system.
* Implement secure file sharing with access controls.
* Add secure group chat for investigation teams.
* Create secure document collaboration tools.
* Implement secure voice calls with automatic encryption.
* Add dead-drop system for sensitive information exchange.

11. Legal and Compliance

* Compliance with Nigeria Data Protection Regulation (NDPR).
* Whistleblower protection under Nigerian laws.
* Partnership with relevant legal bodies.

12. Timeline

* Phase 1: Research and Design – 1 month.
* Phase 2: Development – 3 months.
* Phase 3: Testing and Security Audit – 1 month.
* Phase 4: Launch and Monitoring – 1 month.

13. Conclusion

This system aims to enhance police accountability and protect citizens by providing a secure, efficient way to report police brutality. Continuous updates, stakeholder engagement, and transparent processes will ensure its success and adoption.