National Gender Data Reporting System (NGDRS) - System Requirements Document

1.0 Introduction

This System Requirements Document (SRD) codifies the definitive technical and functional requirements for the National Gender Data Reporting System (NGDRS). It is architected to translate Pakistan's strategic policy goals for combating Gender-Based Violence (GBV) into a functional, secure, and intelligent national data system. This document provides a detailed blueprint to guide the development, deployment, and operation of the NGDRS, ensuring it meets the explicit mandates of the National Commission on the Status of Women (NCSW) and aligns with national and international legal frameworks. The following sections detail the system's strategic vision, user classes, and operational context.

1.1 Purpose

The primary purpose of this SRD is to provide a comprehensive set of technical specifications to guide the development and implementation of the National Gender Data Reporting System (NGDRS). These requirements are derived directly from the mandates of the National Commission on the Status of Women (NCSW) and associated policy documents, including the NCSW Circular for Mandatory Data Reporting, to ensure the system is fit for purpose and aligned with national priorities.

1.2 System Scope

The scope of the NGDRS encompasses the aggregation, validation, and visualization of data on Gender-Based Violence (GBV) and Technology-Facilitated Gender-Based Violence (TFGBV) from across Pakistan. The system is designed to connect Police, Health, Prosecution, and Social Welfare departments at the provincial and federal levels into a single, standardized digital ecosystem for data reporting and analysis. Its scope includes case intake, institutional routing, data triangulation, compliance monitoring, and high-level decision support through an executive dashboard.

1.3 Glossary of Terms

The following table defines key terms and acronyms used throughout this document.| Term | Acronym | Definition || ------ | ------ | ------ || National Gender Data Reporting System | NGDRS | The mission-critical digital infrastructure designed to aggregate, validate, and visualize data on GBV and TFGBV across Pakistan. || National Commission on the Status of Women | NCSW | The primary government body in Pakistan responsible for monitoring the status and rights of women and overseeing the implementation of the NGDRS. || Gender-Based Violence | GBV | An umbrella term for any harmful act perpetrated against a person's will, based on socially ascribed gender differences. || Technology-Facilitated Gender-Based Violence | TFGBV | Acts of violence committed, assisted, or amplified by the use of information and communication technologies or digital media against a person because of their gender. || National Cyber Crime Investigation Agency | NCCIA | The primary federal law enforcement agency responsible for

investigating cybercrimes in Pakistan, replacing the FIA Cyber Crime Wing. || Social Media Protection and Regulatory Authority | SMRA | A new regulatory body established under the PECA 2025 amendments, responsible for content regulation and platform oversight. || Convention on the Elimination of All Forms of Discrimination Against Women | CEDAW | An international treaty adopted by the UN General Assembly that defines what constitutes discrimination against women. || Gender-Based Violence Information Management System | GBVIMS | An inter-agency initiative that provides a standardized methodology for collecting, storing, analyzing, and sharing GBV-related data. || Chinese Wall Security Policy | CWSP | A security model that prevents conflicts of interest by programmatically blocking users from accessing conflicting datasets. || Original Data Warehouse | ODW | A data repository containing full case details, including Personally Identifiable Information (PII), accessible only at the district level with strict controls. || De-identified Data Warehouse | DDW | A data repository containing anonymized and aggregated data, used for federal-level analysis and dashboard reporting. || Prevention of Electronic Crimes Act | PECA | Pakistan's primary legislation governing electronic crimes, including various forms of TFGBV. |

1.4 Referenced Documents

The requirements detailed in this document are informed by and derived from the following core source materials:

- NCSW Circular for Mandatory Data Reporting
- Data Privacy research papers (CWSP/RBAC)
- International frameworks (GBVIMS, CEDAW, Beijing Platform for Action)
- Prevention of Electronic Crimes Act (PECA) and its amendments

2.0 Overall System Description

A clear definition of the system's high-level characteristics is essential for successful implementation. This section establishes the operational context, defines the key actors who will interact with the system, and codifies the foundational constraints that will shape the system's design and architecture. By articulating the vision, users, and environment, we create an unambiguous framework for the technical specifications that follow. The next section will translate these high-level descriptions into a specific architectural philosophy and technology stack.

2.1 System Vision and Core Objectives

The NGDRS shall be engineered not as a passive database, but as a **compliance-driven, survivor-centric enterprise platform** and an **intelligent decision-support system** . It is designed to be an active tool that guides users, enforces compliance, and transforms raw data into actionable intelligence for policymakers and frontline responders.The core objectives of the NGDRS are as follows:

1. **Standardize and Centralize:** To standardize and centralize GBV/TFGBV data reporting across all provinces and relevant departments, creating a single source of truth.
2. **Monitor Compliance:** To serve as the central compliance engine for NCSW to monitor Pakistan's international commitments, including CEDAW and SDG 5.

3. **Provide Actionable Intelligence:** To provide real-time, actionable intelligence to policymakers for the strategic deployment of resources and targeted interventions.
4. **Guide Frontline Officers:** To guide frontline officers through standardized procedures to improve justice outcomes, ensure evidence quality, and enhance survivor support.
5. **Enforce Accountability:** To hold government entities and social media platforms accountable through data-driven transparency and performance monitoring.

2.2 User Classes and Characteristics

The NGDRS will serve several distinct user classes, each with specific roles and levels of interaction:

- **Policymakers (NCSW Chairperson, Prime Minister, Chief Ministers):** High-level users who consume aggregated, anonymized data via the Executive Dashboard for strategic decision-making, trend analysis, and monitoring national performance.
- **District Focal Persons (Police, WPC, Health):** Primary data entry users responsible for the timely and accurate registration of cases and service provision details, mandated to enter data within **24 hours** of a survivor encounter.
- **Data Reviewers (District/Provincial):** Users responsible for data triangulation and validation. They are tasked with running discrepancy audits and flagging mismatches between departmental records before monthly submission.
- **Law Enforcement (NCCIA, Provincial Police):** Users who receive routed case data based on the crime type (digital vs. physical) to initiate and manage investigations.
- **Data Analysts:** Users with restricted access to the De-identified Data Warehouse (DDW) for research, trend analysis, and generating statistical reports. They are programmatically blocked from accessing any Personally Identifiable Information (PII).
- **System Administrators:** Technical users with privileged access, responsible for system maintenance, security management, user account provisioning, and ensuring operational uptime.

2.3 Operating Environment

The NGDRS is a national-level system architected for a diverse and challenging operational environment.

- **Hosting Infrastructure:** The system will be hosted on a **Government Private Cloud (NTC)** to ensure data sovereignty, security, and compliance with government IT policies.
- **Connectivity Solution:** To support users in districts with poor or intermittent internet connectivity, the system will be implemented as a Progressive Web App (PWA) with an **Offline-First Architecture** . This will allow frontline users to enter and save data locally on their devices. The data will be encrypted at the device level and automatically synchronized with the central server once a stable internet connection is available.

2.4 Design and Implementation Constraints

The development and deployment of the NGDRS must adhere to the following critical constraints:

- **Mandatory Deadline:** The system must be fully operational and ready to accept its first mandatory data submission by **January 28, 2026** .

- **Interoperability:** The system must be built with a robust API gateway to ingest data from external systems, including the NCCIA's case management system, national helplines (1043/1737), and provincial prosecution databases, to ensure a holistic view of the justice lifecycle.
- **Privacy by Design:** The architecture must enforce strict data privacy and security principles from the ground up, treating survivor confidentiality as a non-negotiable requirement.

3.0 System Architecture and Technology Stack

A well-defined architecture is the foundation of a robust and effective system. This section outlines the core technical framework, design philosophies, and specific technologies chosen to ensure the NGDRS is scalable, secure, and capable of fulfilling its role as an intelligent decision-support system. These architectural choices are driven by the principles of privacy, federated control, and performance. The next section will detail the logic and intelligence built upon this architecture, which constitutes the system's "brain"—the knowledge base and rules engine.

3.1 Architectural Philosophy

The system's design is guided by two foundational architectural philosophies that directly support the "Privacy by Design" constraint:

- **"Privacy by Design":** This principle dictates that survivor privacy and data security are not add-on features but are foundational elements integrated into every component of the system from its inception. This includes end-to-end encryption, strict access controls, and data minimization techniques.
- **"Federated Data Control":** As a direct implementation of "Privacy by Design," this approach ensures that the most sensitive data, particularly personally identifiable information (PII), remains at the district level where it is collected. Only anonymized, hashed identifiers and de-identified data are synchronized to the federal database for aggregation and analysis, minimizing the risk of large-scale data breaches.

3.2 Technology Stack Specification

The selected technology stack prioritizes open-source standards, scalability, and rapid deployment to meet the system's aggressive timeline and long-term operational demands. The following table specifies the technologies selected for the key components of the NGDRS architecture.| Component | Specified Technology || ------ | ------ || Backend | Node.js (NestJS) or Python (Django) microservices || Relational Database | PostgreSQL || Geospatial Database | PostGIS || Frontend | React.js / Next.js || Dashboard Engine | PowerBI Embedded |

3.3 Data and Security Architecture

The security architecture is designed to provide multi-layered protection for sensitive survivor data.

- **Encryption:** All data at rest within the system's databases must be encrypted using the **AES-256 encryption** standard.

- **Identity Management:** The system must utilize **Zero-Knowledge Proofs** for survivor identity management. This cryptographic method allows the system to verify identities without ever storing or transmitting PII at the federal level, ensuring maximum privacy.
- **Data Warehousing:** A two-tiered data warehouse structure is required to enforce the principle of federated data control:
- **Original Data Warehouse (ODW):** This warehouse is located at the district or origin level and contains the full, unredacted case details, including PII. Access is strictly controlled and limited to authorized personnel within that jurisdiction.
- **De-identified Data Warehouse (DDW):** This federal-level warehouse contains only anonymized and aggregated data. It powers the national dashboards and analytical functions. PII is programmatically excluded from this warehouse.

4.0 System Knowledge Base and Rules Engine

This section details the "intelligence" of the NGDRS. By encoding legal, procedural, and taxonomic knowledge directly into the system, the platform transforms from a passive data repository into an active "digital supervisor" that guides users, prevents procedural errors, and enforces compliance with legal and operational mandates. The next section will demonstrate how this embedded knowledge is applied in the step-by-step processing of a case from intake to resolution.

4.1 Legal & Juridical Knowledge Base

The system's rules engine must encode Pakistani law to provide real-time guidance and prevent critical procedural errors.

- **Criminal Law Mapping:** The system must include a mapping table that links user-selectable crime descriptions to the corresponding legal sections of the **Pakistan Penal Code (PPC)** and the **Prevention of Electronic Crimes Act (PECA)** .
- *Example:* A selection of "Sharing Intimate Images" must be automatically tagged with **PECA Section 21** .
- *Example:* A selection of "Deepfake" must be automatically tagged with both **PECA Section 21** and **Section 16** .
- **Compoundable vs. Non-Compoundable Logic:** The system must contain a hard-coded rule to **block** the "Mediation/Reconciliation" workflow for **Non-Compoundable** offenses, which cannot be legally settled or compromised.
- **Blocked for:** Rape (Section 375/376) and Sexual Abuse (Section 377A).
- **Allowed for:** Sexual Harassment (Section 509).
- **Jurisdictional Routing Logic:** The system must contain logic to automatically distinguish between cyber and physical crimes for routing to the correct investigative agency.
- *Rule:* If a crime is *only* digital (e.g., cyberstalking), the system must route the complaint directly to the **NCCIA** .
- *Rule:* If a crime involves physical harm facilitated by technology, the system must trigger a joint alert to both **Provincial Police** and **NCCIA** .

4.2 Typology & Taxonomy Knowledge Base

To ensure data consistency and interoperability, the system must implement standardized classification systems for all categorical data.

- **GBVIMS Standardization:** All relevant dropdown menus for classifying GBV incidents must align with the **6 Core GBV Types** defined by the Gender-Based Violence Information Management System (GBVIMS):
- Rape
- Sexual Assault
- Physical Assault
- Forced Marriage
- Denial of Resources
- Psychological/Emotional Abuse
- **TFGBV Taxonomy:** The system must include the full range of NCSW-mandated digital violence codes for classifying technology-facilitated crimes, including:
- **TF-A1:** Cyberstalking / persistent digital monitoring
- **TF-A2:** Doxxing (leak of personal info)
- **TF-A3:** Threats / extortion
- **TF-A4:** Deepfake sexual content
- **TF-A5:** Non-consensual image/video sharing
- **TF-A6:** AI voice cloning coercion
- **TF-A7:** Online harassment / mobbing
- **TF-A8:** Sextortion/blackmail
- **TF-A9:** Location-based targeting (GPS stalking)

4.3 Operational Knowledge Base (SOPs & Referrals)

The system must embed Standard Operating Procedures (SOPs) into its workflow logic to guide users and enforce best practices.

- **"No Wrong Door" Referral Directory:** The system must contain a geo-tagged directory of verified service providers, including shelters, legal aid organizations, and hospitals.
- *Logic Example:* If a case is registered for a survivor in Multan, the system must auto-populate a referral list with the contact information for the nearest **Dar-ul-Aman (Shelter)** and the relevant **Women Protection Officer (WPO)** .
- **Medical & Forensic Protocols:**
- The system must automatically trigger a "Medical Exam" checklist if "Rape" is selected as the crime type.
- The system must generate a critical alert if the medical exam is not flagged as conducted within **72 hours** of the incident.
- The system must flag or **block** any data entry related to the **"Two-Finger Test,"** explicitly noting that the practice is illegal and unconstitutional.
- **Safety Assessment Tools:** The system must include a **"Lethality Assessment"** module to identify high-risk situations.

- *Rule:* If a victim's report includes keywords like "Choking" or "Weapon Display," the system must calculate a **"High Risk"** score and trigger an immediate rescue alert to relevant authorities.

4.4 International Reporting Knowledge Base

To support the NCSW's compliance monitoring mandate, the system must contain a knowledge base to map local case data to international reporting indicators.

- **CEDAW & BPfA Compliance:** The system must be able to tag every case with relevant indicators, such as **"SDG 5.2.1: Proportion of ever-partnered women subjected to physical/sexual violence."** This functionality is essential for the automated generation of the annual CEDAW Compliance Report.

5.0 Data Lifecycle and Workflow Requirements

This section specifies the workflow requirements that will digitize and enforce the official Standard Operating Procedures (SOPs), creating a consistent, auditable "golden thread" for every case. This structured lifecycle, from initial report to final resolution, ensures compliance, accountability, and high-quality data at every step. The next section will detail the specific system modules and user interfaces that are powered by this structured workflow.

5.1 Step 1: Intake and Digital Registration

1. **Timing:** All data related to a survivor encounter must be entered into the NGDRS within **24 hours** .
2. **System Action:** Upon the creation of a new case, the system must perform the following actions automatically:
3. Generate a unique, anonymized hash that will serve as the **Case_ID** .
4. Force the data entry user to select from standardized dropdowns for Crime Type (e.g., GB-PH, GB-SX) and TFGBV Code (e.g., TF-A1, TF-A4) to ensure data consistency.

5.2 Step 2: Automated Institutional Routing

- **Logic:** The system must automatically analyze the Crime_Type field and route the case data or generate alerts for the appropriate agencies.
- **Physical Violence:** Route the case to the Provincial Police & Prosecution dashboard.
- **Digital Violence (TFGBV):** Route the case directly to the **NCCIA** dashboard for specialized investigation.
- **Online Content Removal:** If the "Online Harm/Content" flag is checked, a sub-ticket must be routed to the **SMRA** to trigger their mandated 24-hour content takedown process.

5.3 Step 3: Data Triangulation and Validation

- **System Action:** Prior to the monthly submission deadline, the system must run an automated **Discrepancy Audit** to validate the data across departments.
- **Rule:** The system must enforce the following core validation rule: If the Police department in District X reports '5 Rape Cases' for a given month, but the Health

department reports '0 Medico-Legal Exams' for the same period, the system must flag a **Data Mismatch Alert** .

- **Remedy:** Any record flagged with a data mismatch must be locked from submission and returned to the originating user for rectification. The user will have **72 hours** to resolve the discrepancy.

5.4 Step 4: Submission and Automated Alerting

1. **Frequency:** Monthly data reports from all districts are due by the **10th** of the following month.
2. **"Red Zone" Logic:** Upon successful submission, the system must immediately analyze the data for each district and calculate two risk thresholds:
3. **Density:** Cases / 100,000 population > 50
4. **Velocity:** >25% increase in reported cases compared to the previous month.
5. **Trigger:** If either of these conditions is met, the system must automatically tag the district as a **RED ZONE** and send an immediate SMS and Email alert to the respective Chief Secretary and the NCSW Chairperson.

6.0 Functional Modules and Features

The system's functional modules are the primary interfaces through which users will interact with its data and intelligence. The features detailed below were selected to transform raw information into actionable insights for intervention, accountability, and evidence-based policy-making, catering to the specific needs of different user classes from frontline officers to national leaders. The next section will detail the specific data schemas and taxonomies required to power these functional modules.

6.1 National Executive Dashboard

The NCSW Executive Dashboard is the system's primary tool for high-level analysis and decision-making. It will consist of five main views:

- **View 1: National Command Center**
- **Purpose:** To provide an immediate "health check" of women's safety nationwide, enabling real-time, actionable intelligence (Objective 3).
- **Metrics/Widgets:**
- Total Incident Volume (KPI Card)
- Red Zone Counter (KPI Card)
- TFGBV Ratio (Donut Chart)
- Reporting Compliance (Bar Chart)
- **View 2: The Justice Funnel**
- **Purpose:** To visualize attrition in the justice system from report to conviction, pinpointing systemic failures to enforce accountability (Objective 5).
- **Metrics/Widgets:**
- **Sankey Diagram** visualizing the flow of cases from Reported to Conviction.
- Conviction Rate (Gauge Chart)
- Reasons for Closure (Treemap)
- **View 3: TFGBV & Platform Accountability**

- **Purpose:** To monitor digital crime trends and hold social media platforms accountable for their response to online harms (Objective 5).
- **Metrics/Widgets:**
- Crime Morphology (Horizontal Bar Chart by TF_Code)
- Platform Leaderboard (**Matrix Table**) tracking Total Complaints, Takedown Success %, and Average Response Time for platforms like TikTok, Meta, and X.
- **View 4: Service Provision & Survivor Support**
- **Purpose:** To monitor the provision of essential services and ensure standardized procedures are followed to improve survivor support (Objective 4).
- **Metrics/Widgets:**
- The Service Gap (**Radar Chart**) visualizing gaps across Medical, Legal Aid, Shelter, and Psychosocial services.
- Triangulation Check (Status Indicator) to flag data mismatches between departments.
- **View 5: Geospatial Risk Map (GIS Module)**
- **Purpose:** To provide an interactive, geographic visualization of GBV hotspots, enabling strategic resource deployment (Objective 3).
- **Metrics/Widgets:**
- An interactive **Chloropleth Map** of Pakistan, with districts shaded according to risk level: Green (<20 cases/100k), Amber (20-50 cases/100k), and Red (>50 cases/100k).
- Clicking on a district must open a detailed profile with a crime breakdown and focal person details.

6.2 Reporting and Compliance Module

This module will provide automated reporting features to ensure compliance with national and international obligations.

- **One-Click "CEDAW Report":** A feature that allows authorized users to generate a pre-formatted PDF summary of all indicators required for Pakistan's periodic review to the UN Committee on the Elimination of Discrimination against Women.
- **Automated "Chief Secretary Letter":** A feature that automatically generates a draft non-compliance notification letter, addressed to the relevant Chief Secretary, for districts that miss the monthly reporting deadline.

6.3 Advanced (Production Grade) Features

To enhance the system's effectiveness and usability, the following advanced features must be included:

- **AI-Assisted Classification:** An NLP model will scan free-text case descriptions entered by officers and suggest the correct standardized TFGBV code (e.g., text containing "threat to leak video" will prompt a suggestion for **TF-A8 Sextortion/blackmail**).
- **Deepfake Detection Flag:** An API integration will be implemented to flag uploaded video evidence for "Potential AI Manipulation," providing an early warning to investigators.
- **Offline "Store & Forward" PWA:** As detailed in the operating environment, a Progressive Web App will allow users in low-connectivity areas to enter data offline,

which is then encrypted locally and synchronized automatically when a connection is restored.

7.0 Data Schema and Standardization Requirements

A standardized data model is the bedrock of data integrity and system-wide interoperability. This section defines the foundational data structures and taxonomies that ensure data is collected and stored consistently across all departments and provinces. This standardization is what makes meaningful national-level analysis possible. The next section will outline the stringent security and privacy protocols necessary to protect the sensitive data defined here.

7.1 Database Schema Model

The system's relational database must include the following core tables with the specified key fields:

- **Survivor_Cases**
- Case_ID (Primary Key, Anonymized Hash)
- Date_Reported
- Province_ID
- District_ID
- **Incident_Details**
- FK_Case_ID (Foreign Key to Survivor_Cases)
- Crime_Code
- Location_Type
- Perpetrator_Type
- **TFGBV_Specifics**
- FK_Case_ID (Foreign Key to Survivor_Cases)
- Platform
- TF_Code
- Takedown_Requested
- Takedown_Time_Hours
- **Justice_Funnel**
- FK_Case_ID (Foreign Key to Survivor_Cases)
- Current_Stage (Enum: FIR Registered to Conviction)
- Attrition_Reason
- **Service_Provision**
- FK_Case_ID (Foreign Key to Survivor_Cases)
- Medical_Aid (Y/N)
- Psychosocial_Support (Y/N)
- Legal_Aid (Y/N)
- Shelter_Provided (Y/N)

7.2 Data Dictionaries and Standardized Taxonomies

All categorical data fields within the system must use standardized, centrally-managed dropdown lists (enumerations) to eliminate data entry errors and ensure consistency.**Violence Category Codes** | Code | Category | | :--- | :--- | | GB-PH | Physical | | GB-SX | Sexual | |

GB-EC | Economic | | GB-PY | Psychological | | GB-FM | Forced Marriage | | GB-TR | Trafficking | | GB-FE | Femicide |**TFGBV Type Codes** | Code | TFGBV Sub-Type | | :--- | :--- | | TF-A1 | Cyberstalking / persistent digital monitoring | | TF-A2 | Doxxing (leak of personal info) | | TF-A3 | Threats / extortion | | TF-A4 | Deepfake sexual content | | TF-A5 | Non-consensual image/video sharing | | TF-A6 | AI voice cloning coercion | | TF-A7 | Online harassment / mobbing | | TF-A8 | Sextortion/blackmail | | TF-A9 | Location-based targeting (GPS stalking) |

8.0 Security and Privacy Requirements

The paramount importance of security and privacy cannot be overstated in a system designed to handle highly sensitive data related to survivors of violence. These requirements are non-negotiable and are architected to build trust with both users and survivors, protect individuals from re-victimization, and prevent any misuse of the collected data. The next section will outline the deadlines and compliance actions required to bring this secure and robust system to fruition.

8.1 Data Access Control

- **Chinese Wall Security Policy (CWSP):** The implementation of a **CWSP** is a core requirement. This policy creates a mandatory, programmatic separation between conflicting datasets to prevent unauthorized access.
- **Implementation:** A user role such as "Data Analyst" must be granted access to the **De-identified Data Warehouse (DDW)** for analytical purposes but must be technically and programmatically **blocked** from accessing the **Original Data Warehouse (ODW)** , which contains PII. This ensures that analytical functions can be performed without compromising survivor confidentiality.

8.2 Data Anonymization and De-identification

- **K-Anonymity:** The system must enforce **K-Anonymity** principles to prevent the re-identification of individuals from aggregated data.
- **Application Rule:** When generating public-facing visualizations like heatmaps, if a specific geographic area (e.g., a village or a small neighborhood) has fewer than 5 reported cases, the system must automatically aggregate the data to a higher geographic level (e.g., Tehsil or District) or suppress pinpoint locations. This prevents deductive disclosure of a survivor's identity.
- **Dashboard Granularity:** All dashboards and reports accessible at the federal level must never expose survivor names, contact information, or exact addresses. The lowest level of geographic granularity permitted for national-level reporting will be the District level.

9.0 Implementation Mandates and Timeline

This final section serves as the call to action, outlining the official timeline and compliance directives from the NCSW. These mandates establish the development and adoption of the NGDRS as a national priority with clear, non-negotiable deadlines for all involved entities.

9.1 Mandatory Compliance

As per the NCSW Circular for Mandatory Data Reporting, providing data to the NGDRS in the prescribed digital format is **mandatory** for all specified provincial and federal entities, including Police, Health, Prosecution, and Social Welfare departments. Non-compliance with the reporting schedule or format will be formally referred to the respective Chief Secretary or Federal Secretary for immediate corrective action.

9.2 Key Submission Deadlines

The implementation of the NGDRS is bound by the following critical deadlines:

- **System Go-Live:** The NGDRS must be fully operational, tested, and ready to accept data submissions before the first reporting deadline.
- **First Mandatory Submission Deadline: January 28, 2026** .
- **Ongoing Monthly Reports:** Subsequent monthly reports are due by the **10th of each month** .

This system will transform the NCSW from a passive observer into an active monitoring body, armed with the data evidence required to hold police, platforms, and provincial governments accountable.