01. Data Handling Policy:

- The Grievance Redressed System (GRS) is committed to ensuring the privacy and security of user data.
- All data collected through the GRS will be handled in accordance with applicable data protection laws and regulations.
- The GRS will only collect and process personal data necessary for the purpose of resolving grievances and ensuring effective redressed.
- User data will be handled securely, protected from unauthorized access, and used solely for the intended purposes of the GRS.
- The GRS will implement appropriate technical and organizational measures to safeguard user data from loss, misuse, or unauthorized disclosure.
- User data will be retained for the duration necessary to fulfill the purposes for which it was collected or as required by law.

02. PII Data Collection and Distribution Policy:

2.1 Collection of Personal Identifiable (PI) Data:

We collect personal information from end users and administrative officers at various times to provide our services. The process of collecting personal data (PI) is described below.

1. Complaint Registration: We collect the following information, which is not compulsory, from the complainant for grievance registration: name, mobile number, and email, date of birth, gender, educational qualification, professional qualification, NID number, country, and address. Complainants can also submit grievances anonymously without providing personal information.
2. Administrative User Registration: We collect the user's office ID and password for administrative user registration.
3. Grievance Submission: When submitting a complaint, we collect the following information, if available: mobile number, email, grievance submission office, subject of the grievance, description, and any relevant grievance-related document files.

2.2 Use of PI Data:

1. Service Provision: Collecting personal information, such as name, mobile number, email, address, and other relevant details, is necessary to effectively provide the

grievance redressed service. This information helps identify and contact the complainant, maintain accurate records, and facilitate the resolution process.

2. Authentication and Security: To prevent unauthorized access to the system and ensure account security, users, including administrative officers, may be required to provide personal information such as office ID, password, and other relevant authentication credentials.

3. Communication and Notification: Personal contact details like mobile numbers and email addresses are collected to facilitate communication between system administrators and complainants. This allows for updates on the grievance resolution process, acknowledgment of receipt, and any additional information related to the complaint.

4. Legal and Regulatory Compliance: Collecting personal information, including NID numbers or other identification details, may be necessary to comply with legal and regulatory requirements specific to the grievance redressed system. This ensures the system operates in accordance with applicable laws and regulations.

5. Anonymous Submissions: Some grievance redressed systems allow users to submit complaints anonymously without providing personal information, thus maintaining privacy while still accessing the system's services.

It is essential for the privacy policy to outline the specific types of personal information collected, the purpose of collection, and how the information is stored, used, and protected. This helps users understand how their data will be handled and assures them that their privacy is respected within the system.

3. Non-PII Data Collection and Distribution Policy:

3.1 Collection of Non- Personal Identifiable (PI) Data:

We also collect non-personally identifiable (non-PI) data at certain moments, as described below:

- Feedback and Ratings: Users can provide feedback on closed grievances after they have been resolved by the GRO officer.
- Suggestions for Improvement: Users can provide suggestions to enhance the service.

3.2 Use of PI Data:

1. Privacy Protection: Collecting non-PI data ensures that individuals' personal and sensitive information is not disclosed or exposed, protecting users' privacy rights and preventing potential misuse of their personal data.
2. Anonymity: Non-PI data allows individuals to provide feedback, ratings, and suggestions without revealing their identity. This anonymity encourages users to express their honest opinions and share their experiences freely.
3. Service Improvement: Collecting feedback and suggestions is crucial for enhancing service quality. Non-PI data allows organizations to gather valuable insights, identify areas for improvement, and make necessary changes to increase user satisfaction.
4. Aggregated Analysis: Aggregating and analyzing non-PI data helps identify broader patterns, trends, and issues within the grievance redressed system. This analysis enables data-driven decision-making, prioritization of improvement areas, and overall system efficiency enhancement.

Data Manipulation: Users can download data in formats such as xlsx, csv, and pdf. They can also print various system data, including user guidelines, citizen charters, offline grievance submission forms, as well as dashboard and report information.

4.0 License Policy:

- The Grievance Redressed System (GRS) operates under a license that governs its usage, access, and functionalities.
- Users of the GRS must comply with the terms and conditions outlined in the license agreement.
- Any unauthorized use, modification, or distribution of the GRS, its software, or associated materials is strictly prohibited.
- The GRS reserves the right to take appropriate legal action against individuals or entities found to be in violation of the license policy.

5.0 Cookie Policy:

- The GRS may use cookies or similar technologies to enhance user experience and facilitate system functionalities.

- Cookies are small text files stored on users' devices that collect certain information to personalize and improve user interactions with the GRS.
- Users have the option to accept or decline cookies through their browser settings.
- The GRS may use both session cookies (temporary) and persistent cookies (stored for a longer duration) for various purposes, including authentication, preferences, and analytics.

6.0 Authentication Policy (Security Policy):

- The GRS employs robust authentication mechanisms to ensure the security and integrity of user accounts.
- Users may be required to create unique credentials, such as usernames and passwords, to access the GRS.
- The GRS will implement industry-standard security measures to protect user authentication information from unauthorized access or disclosure.
- Users are responsible for maintaining the confidentiality of their authentication credentials and are encouraged to use strong, unique passwords.