City Data Policy of

Solapur Municipal Corporation

2019

Contents

1. Preamble

Asset and value potentials of data are widely recognized at all levels. Data collected or developed through public investments, and services when made publicly available and maintained over time, their potential value could be more fully realized. There has been an increasing demand by the community, that such data collected' with the deployment of public funds should be made more readily available to all, for enabling rational debate, better decision making and use in meeting civil society needs.

Principle 10 of the United Nations Declaration on Environment and Development

"Each individual shall have appropriate access to information concerning the environment that is held by public authorities, and the opportunity to participate fry the decision making process. Stares shall facilitate and encourage public awareness and participation by making information widely available!"

Section 4(2) of the night to Information Act, 2005 reads:

"It states that every public *authority* should *take steps in to* provide information to the *public regular* intervals through various *means* of *communication, including internet, so that* the *public* have *minimum resort to the use of* this Act *to obtain information"*

1.2 The principle of data sharing accessibility include Openness, Flexibility , Transparency, conformity, protection of Intellectual Property Right, , Formal Responsibility, interoperability, Quality, Security, Efficiency, Accountability , Sustainability and Privacy.

1.3 A large quantum of data generated using public funds by various organizations and institutions in the country remains inaccessible to civil society, although most of such data may be non-Sensitive in nature and could be used by public for scientific, economic and developmental purposes. Efficient sharing of data among data owners and inter-and-intra governmental agencies along with data standards and interoperable systems is the need of the hour. Hence, there was a need to formulate a policy on National Data Sharing and Accessibility which could provide an enabling provision and platform for proactive and open access to the data generated through public funds available with various ministries/departments/organizations of Government of India. In purview of the same, Solapur Municipal Corporation (hereafter, SMC) has decided to endorse the National Data Sharing and Accessibility Policy and developed the Open data portal. The policy is designed to promote data sharing and enable access to Government owned data for planning and development.

2. Definitions

2.1 Data

Data means a representation of information, numerical compilations and observations, documents, facts, maps, images, charts, tables and figures, concepts in digital and/or analog form.

2.2 Data Archive

A place where machine-readable data are acquired, manipulated, documented, and distributed to others for further analysis and consumption.

2.3 Data Generation

Initial generation / collection of data or subsequent addition of data to the same specification.

2.4 Data set

A named collection of logically related features including processed data or information.

2.5 Geospatial Data

All data which is geographically referenced

2.6 Information

Processed data

2.7 Metadata

The information that describes the data source and the time, place, and conditions under which the data were created.Metadata informs the user of who, when, what, where, why, and how data were generated. Metadata allows the data to be traced to a known origin and know quality.

2.8 Negative list

Non sharable data as declared by the departments / organizations

2.9 Restricted Data

Data which are accessible only through a prescribed process of registration and authorization by respective departments / organizations.

2.10 Sensitive data

Sensitive data as defined in various Acts and rules of the Government of India & Government of Maharashtra & Maharashtra Municipal Act.

2.11 Sharable data

Those data not covered under the scope of negative list and non-sensitive in nature

2.12 Standards

Any application that embeds data handling functions (e.g., data collection, management, transfer, integration, publication, etc.) and operates on data in a manner that complies with data format and data syntax specifications produced and maintained by open, standards bodies.

3. Need for the Policy

Evidence-based Planning of socio-economic development processes rely on quality data. There is a general need to facilitate sharing and utilization of the large amount of data generated and residing among the entities of the Government departments and municipal corporations. This would call for a policy to leverage these data assets which are disparate. The current regime of data management does not enable open sharing of Government owned data with other arms of the government nor does it expect proactive disclosure of sharable data available with data owners. Such regimes could lead to duplication of efforts and loss of efficiency of planning of activities focused on development. Efficient sharing of data among data owners and inter and intra governmental agencies and with public calls for data standards and interoperable systems. Hence, Data Sharing and Access Policy of SMC aims to provide an enabling provision and platform for providing proactive and open access to the data generated through public funds& public revenue available with various departments of SMC.

4. Objectives

The objective of this policy is to facilitate access to the Municipal Corporation owned shareable data and information in both human readable and machine readable forms through a network all over the country in a proactive and periodically updatable manner, within the framework of various related policies, Acts and rules of Government of India, thereby permitting wider accessibility and use of public data and information.

5. Scope of this Policy

The Data Sharing and Accessibility Policy of SMC will apply to all data and information created, generated, collected and archived using public funds provided by Government Departments/ Municipal corporations directly or through authorized agencies by various Ministries / Departments /Organizations / Agencies and Autonomous bodies.

6. Benefits of the data sharing policy

6.1 Maximized use : Ready access to government owned data will enable more extensive use of a valuable public resource for the benefit of the community.

6.2 Avoiding duplication : By sharing data, the need for separate bodies to collect the same data will be avoided resulting in significant cost savings in data collection.

6.3 Maximized integration : By adopting common standards for the collection and transfer

of data, integration of data sets may be feasible.

6.4 Ownership information : The identification of owners for the principal data sets provide information to users to identify those responsible for implementation of prioritized data correction programs and development of data standards.

6.5 Better decision-making : Data and information facilitates making important decisions without incurring repetitive costs Ready access to existing valuable data is essential for many decision making tasks such as protecting the environment, development planning, managing assets. Improving ease of living conditions, national security and controlling disasters.

4.6 Equity of access: A more open data transfer policy ensures better access to all bonafide users.

7. Data Classification

Different types of data sets generated both in geospatial and non-spatial form by different ministries departments are to be classified as shareable data and non-shareable data. The types of data produced by a statistical system consists of derived statistics like national accounts statistics, indicators like price index, data bases from census and surveys. The geospatial data however, consists primarily of satellite data, maps, etc. In such a system, it becomes important to maintain standards in respect of metadata, data layout and data access policy. All departments of SMC will prepare the negative list within six months of the notification of the policy, which will be periodically reviewed by the oversight committee.

7.1 Review Committee

1. Hon. Commissioner
2. Programmer / Nodel Officer
3. Concerned Departments Data Coordinator
4. Chief Data Officer

8. Data Categorization

8.1. Data will be categorized into two broad categories:

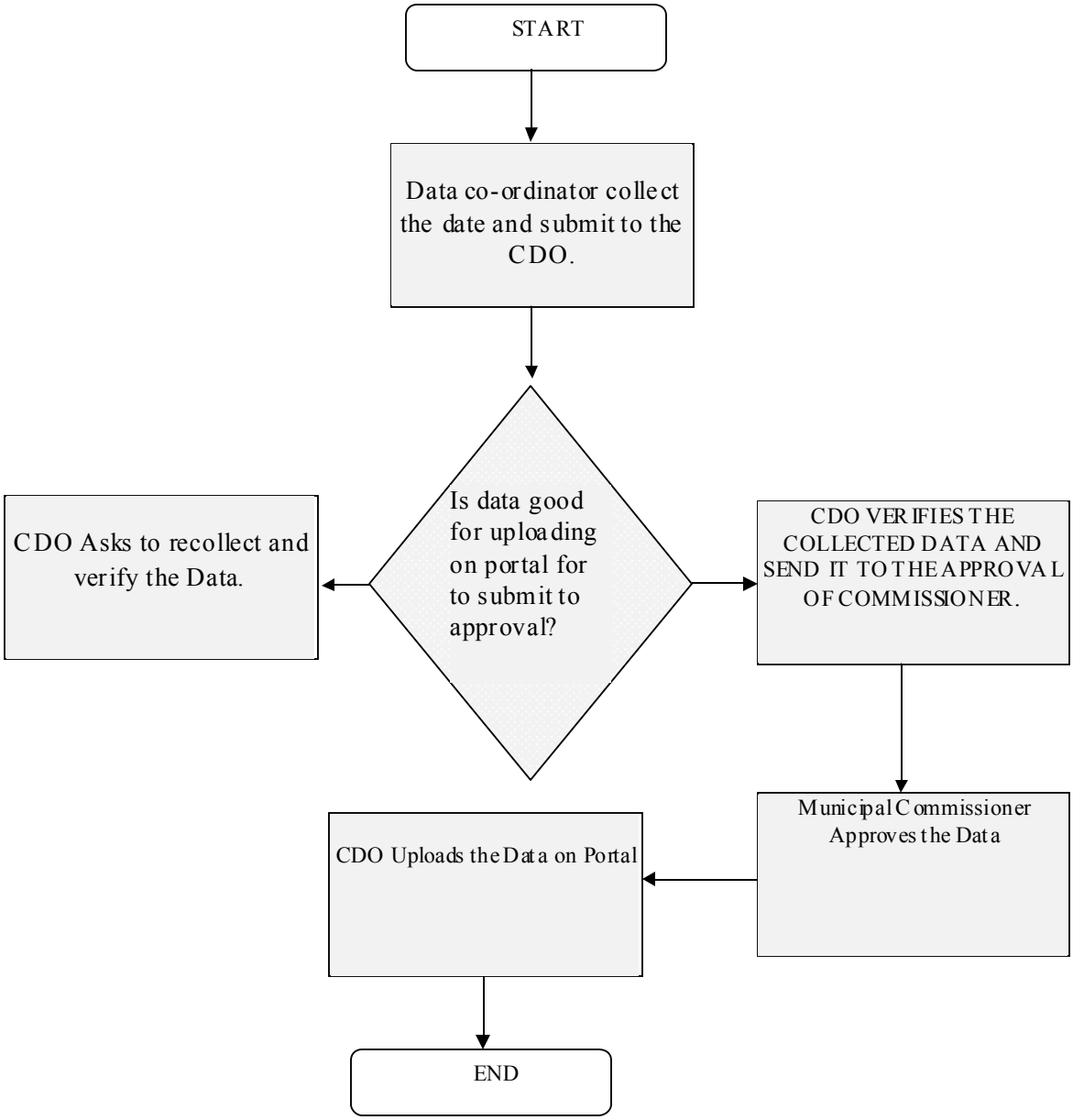
8.1 Personal Data: Personal data means data consisting of information which is related to a living individual who can be identified from that information (or from that and other information in the possession of the data users), including any expression of opinion about the individual but not any indication of the intention of the data user in respect to that individual.' 'Data' is defined as information recorded in a form in which it can be processed by equipment operating economically in response to instructions given for that purposes.

8.2. Non Personal Data: Non-personal data also refers to anonymous information/data, namely information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In other word, anonymization means excluding any personal identifiers from data sets.

8.3. **Personal and Non Personal Data will be classified into following category:**

Classification	Class	Definition
Level-1	Public	Data available for public consumption and use.
Level-2	Internal Use	Information which could only be disclosed to Municipal Corporation employees for managing operations or delivery of public services on day to day basis.
Level-3	Sensitive	Data regulated by any City/ State/Central law or regulation like privacy etc.
Level-4	Protected	Data which needs to be protected for e.g. Identity of citizens and disclosure /notification needs to be issued by municipal corporation in case of any breach or loss of data.
Level-5	Restricted	Data which could lead to threat to life or loss of public assets or critical infrastructure.

9 Data Flow / Approval Framework



10. Types of Access

10.1 Open Access

Access to data generated from public funding should be easy, timely, user-friendly and web-based without any process of registration / authorization.

10. 2 Registered Access

Data sets which are accessible only through a prescribed process of registration/authorization by respective departments / organizations will be available to the recognized institutions / organizations / public users, through defined procedures.

10.3. Restricted Access

Data declared as restricted, by Government of India & Government of Maharashtra policies, will be accessible only through and under authorization.

11 Technology for sharing and Access

A state-of-the-art data warehouse and data archive with online analytical processing (OLAP) capabilities, which includes providing, a multi-dimensional and subject oriented view of the database needs to be created. This integrated repository of data portals of various ministries / departments as a part of data.gov.in, will hold data and this repository over a period of time will also encompass data generated by various Central Government, State Governments and Authorities within SMC limit. The main features of the data warehouse need to include:

(a) User friendly interface

(b) Dynamic/pull down menus

(c) search based Report

(d) Secured web access

(f) Complete Metadata

(g) Parametric and Dynamic report in exportable format

12 Legal framework

Data will remain the property of the agency/department/ ministry/ entity which collected them and reside in their IT enabled facility for sharing and providing access. Access to data under this policy will not be in violation of any Acts and rules of the Government of India in force. Legal framework of this policy will be aligned with various Acts and rules covering the data& Government of Maharashtra.

13 Data Archival and Retention

E-Files/records may be digitized by any one of the categories:

(1) Category-I (e-Files/records to preserved permanently which are of historical importance) – For 10 years, it will be kept in the Department's server and thereafter transferred other available physical storage formats such as Tapes, hard-drives, Storages etc.

(2) Category –II (e-Files/records of secondary importance and have a reference value for a limited period) – 10 years on the Department's server. In exceptional cases, if the record is required to be retained beyond 10 years it will be upgraded to Category-I.

Data will be stored in the main database for 6 Months in a live state so that whenever a report needs to be generated, the data will be extracted from main database. Data older than 6 months will be archived. If report duration extends beyond 6 months, the data will be retrieved from archrivals to generate the report.

14 Pricing

Pricing of data, if any, would be decided by the data owners and as per the standard government policies. All Ministries /Departments will upload the Pricing policy of the data under registered and restricted access within three months of the notification of the policy. A broad set of parameters would be standardized and provided as guidelines for the use of data owners.

15 Standard Operating Procedures (SOP)

15.1 Standard Operating Procedures for Data Collection

If the request is received from external agency

1. If the request is received from external agency, it should be directed to Chief Data Officer (CDO).
2. Depending on the requested data or the data which need to be collected, the CDO shall direct the request to Data Coordinator (DC) of the concerned department.
3. The Data Coordinator of the concerned departments checks the requested data. If data is available with department, DC shall instruct the concerned personnel to gather the data in requested format.
4. Data coordinator will take approval of data from their HOD
5. If fresh data need to be captured/acquired, the Data Coordinator (DC) in consultation with Chief Data Officer (CDO) shall take appropriate action.

If the request is received from Internal Departments

1. If the request is received from Internal Departments, it can be directed to Data Coordinator of the concerned department.
2. The Data Coordinator of the concerned departments checks the requested data. If data is available with department, DC shall instruct the concerned personnel to gather the data in requested format.
3. If fresh data need to be captured/acquired, the Data Coordinator (DC) in consultation with Chief Data Officer (CDO) shall take appropriate action.

15.2 Standard Operating Procedures for Data Quality Assessment

1. Under the leadership of Hon'ble commissioner, three member committee will be formed comprised of Commissioner, Programmer, Department HOD and Chief Data Officer (CDO).

15.3 Standard Operating Procedures for Stakeholder engagement

1. Head of Department (HoDs) or Data Coordinators of departments will identify the need of data from their respective departments.

2. Biweekly meeting shall be conducted with all Head of Departments or Data Coordinators under the chairmanship of Hon'ble Municipal Commissioner/ Additional Commissioner to understand the needs of data

15.4 Standard Operating Procedures for data collection through field survey

1. Depending on requirement of data, competent agency can be employed to perform field survey

Going forward, all the e-governance IT applications/Systems shall be designed in such a way that manual processes get replaced by automated process without much intervention of humans. As most of process would be automated and handled by an e-mode, data will be available for further analysis.

16 Implementation

i. SMC will design and position a suitable budgetary incentive system for data owners for increasing open access to the sharable data.

ii. An oversight committee will be constituted for facilitating the implementation of the policy and its provisions thereof.

iii) Computer Department(SMC) will constitute a coordination committee for implementation.

17 Budget Provisions

The implementation of Data Sharing and Access Policy of SMC is expected to entail expenditures for both data owners and data managers for analog to digital conversion, field revenue data refinement data storage, quality up-gradation etc. Budgetary provisions and appropriate support for data management for each department would be necessary.

18 Data Archival and Retention

E-Files/records may be digitized by any one of the categories:

(1) Category-I (e-Files/records to preserved permanently which are of historical importance) – For 10 years, it will be kept in the Department's sever and thereafter transferred other available

physical storage formats such as Tapes, hard-drives etc.

(2) Category –II (e-Files/records of secondary importance and have a reference value for a limited period) – 10 years on the Department's server. In exceptional cases, if the record is required to be retained beyond 10 years it will be upgraded to Category-I.

Data will be stored in the main database for 6 Months in a live state so that whenever a report need to be generated, the data will be extracted from main database. Data older than 6 months will be archived. If report duration extends beyond 6 months, the data will be retrieved from archrivals to generate the report.

19 Data Security

S.No.	Security Areas	Specifications
1.	**Physical Security**	• The premises should be physically secured by the SI.
2.	**Network Security**	• Appropriate firewalls, IPS, SSL devices etc. should be used to ensure Networksecurity • The solution should support SSL encryption mechanism for transferring data across network and between client andserver
3.	**System Security**	• Adequate access control procedures should be defined to secure the entire IT system, physically andlogically. • The access controls procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems andservices. • The system should have 2 factor authentication mechanism either through One Time Password (OTP) or soft tokens based technologies for access control and user authentication.

S.No.	Security Areas	Specifications
4.	**Application Security**	• The solution should have appropriate authentication mechanisms • Application user authentication & authorization related transactions should be encrypted. • Operating system should be hardened on which the application is installed. • A web application firewall shall be deployed to secure the web-layer.
5.	**Audit Trails & Logs**	• Event logging should create an accurate record of user activity such as which users accessed which system, and for how long. • The solution should log all types of events especially those related to security
6.	**Data Protection**	• The solution should support SSL encryption mechanism for transferring data across network. • The data transferred across network should be encrypted using Public Key (PKI) Infrastructure. • Complete end point data protection should be provided at client site such that any type of data pilferage using unauthorized copying, storing and emailing could be prohibited. • Access to all system resources including data files, devices, processes and audit files should be provided to the intended users only. • All mobile applications should be designed and developed in a way that it ensures security of the application and data on the device. • Ensure to protect documents by assigning security parameters and criteria in order to provide more effective protection for an electronic document in order to maintain Confidentiality, Authorization, Accountability, Integrity, Authenticity and Non-repudiation.
7.	**Session Management**	• The system should limit to only one session per user or process ID. • The system should put a limit on the maximum time length of an idle session, which should ensure that automatic session termination takes place after expiry of the specific time length. • Mandatory password change after predefined time period

S.No.	Security Areas	Specifications
8.	**Data Warehouse Security**	• Users must not have access to the data warehouse prompt of the application. Access to the data warehouse prompt must be restricted only to the database administrator. • "Super user" rights for the data warehouse must only be given to the administrator and activities of these accounts must be properly logged.
9.	**Application Deployment**	• All unused ports should be blocked at server machines. • The application server should be segregated from internet zone through firewall or other filtering mechanism.
10.	**Information Security Governance**	• The employees working on the project should be made aware of his or her responsibilities with respect to Information Privacy and Information Security. • Employees working on the project shall undergo security awareness training during training.
11.	**Compliance to Security Standards**	• Software/Hardware system should be in compliance with <ISO/IEC 27001:2015>.
12.	**Security Information and Event Management System (SIEM)**	• SI should install SIEM for Real-time analysis of security alerts generated by applications and infrastructure.
13.	**Database Activity Monitoring (DAM)**	• SI should install DAM to monitor all database

20 SOP for data processing and cleaning

20.1 While collecting the electronic data, the IT applications/ IT systems should be developed in such a way that under any circumstances these applications/systems should not accept any garbage/wrong data/null data

20.2 If there is existing data, identify discrepancies which may come from different sources

20.3 The collected data shall be properly processes and cleaned before performing any kind of analysis.

20.4 If needed commercial software available in the market can be used with prior approvals of concern authority

21 SOP for electronic data collection

21.1 The data should be collected in consent with the end user who may be a citizen
or SMC employee

21.2 Data which is not going to be used for any kind of analysis or will not be used for
any communication purpose should not be collected at all.

21.3 Data Security measures mentioned in "Data Security" shall be followed to maintain confidentiality and security of data

22 SOP for data publishing as per Open Data Norms

1. Only data which has been approved by Assessment Committee and Municipal Commissioner shall be uploaded on Open Data Portals.
2. Data sets which are considered to be open by default unless classified as internal, sensitive, protected or restricted shall be uploaded on the Open Data Portals
3. Data sets and feeds must be published with proper metadata. Information about the datasets being published using common data taxonomy/structure shall be uploaded as it helps in providing easy access through Data Platform.
4. Data Sets and feeds should be published in formats specified under NDSAP i.e. Open format. Data should be provided in freely available formats which can be accessed without the need for a software license.
5. Data Sets and Feeds should be machine readable.
6. Following data formats can be used for uploading data on Open Data Portal
   a. CSV (Comma separated values)
   b. XLS (Spread sheet - Excel)
   c. ODS (Open Document Formats for Spreadsheets)
   d. XML (Extensive Markup Language)
   e. RDF (Resources Description Framework)
   f. KML (Keyhole Markup Language used for Maps)
   g. GML (Geography Markup Language)
   h. RSS/ATOM (Fast changing data e.g. hourly/daily)

Commissioner
Solapur Municipal Corporation

Data Sharing and Accessibility Policy of Solapur Municipal Corporation Page No: 17

Annexure1: Open Data Platform for Solapur (SMC DataStore)

Website has to be created which shall provide the following features:

a. Collated access to Resources (datasets/apps) under Departments published in open format

b. It also provides a search & discovery mechanism for instant access to desired datasets.

c. SMC DataStore shall also have a rich mechanism for citizen engagement.

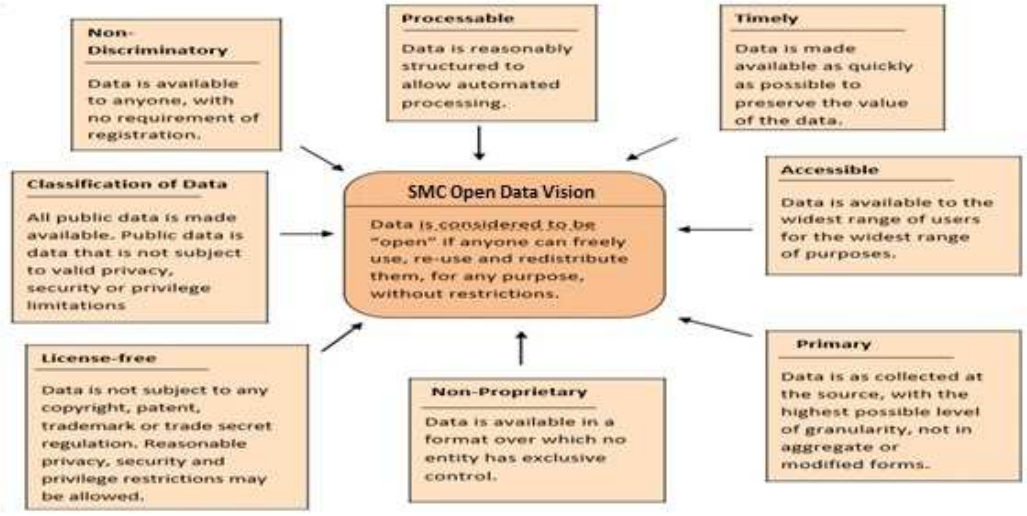
d. Besides enabling citizens to express their need for specific resource (datasets or apps) or API, it also allows them to rate the quality of datasets, seek clarification or information from respective data controller.

Annexure 2: Datasets

Datasets have to be identified (Open Data which can be downloaded by anyone)

Annexure 3: Open Data Platform for Solapur Municipal Corporation (SMC DataStore)

Solapur Data Store to set up to provide collated access to Resources (datasets/apps) under Departments published in open format. It also provides a search & discovery mechanism for instant access to desired datasets. Solapur Data Store to have a rich mechanism for citizen engagement. Besides enabling citizens to express their need for specific resource (datasets or apps) or API, it also allows them to rate the quality of datasets, seek clarification or information from respective data controller.



Annexure 4: NDSAP Implementation

In order to implement open data, SMC has to undertake the following activities:

- Nominate Chief Data Officer
- Nominate Data Contributors
- Identify Datasets
- Publish Resources (Datasets/Apps) on data.gov.in portal
- Prepare Negative List
- Create Action Plan for regular release of datasets on the OGD Platform India
- Monitor and Manage the Open Data Programme of the Department

Commissioner
Solapur Municipal Corporation

Data Sharing and Accessibility Policy of Solapur Municipal Corporation Page No: 21