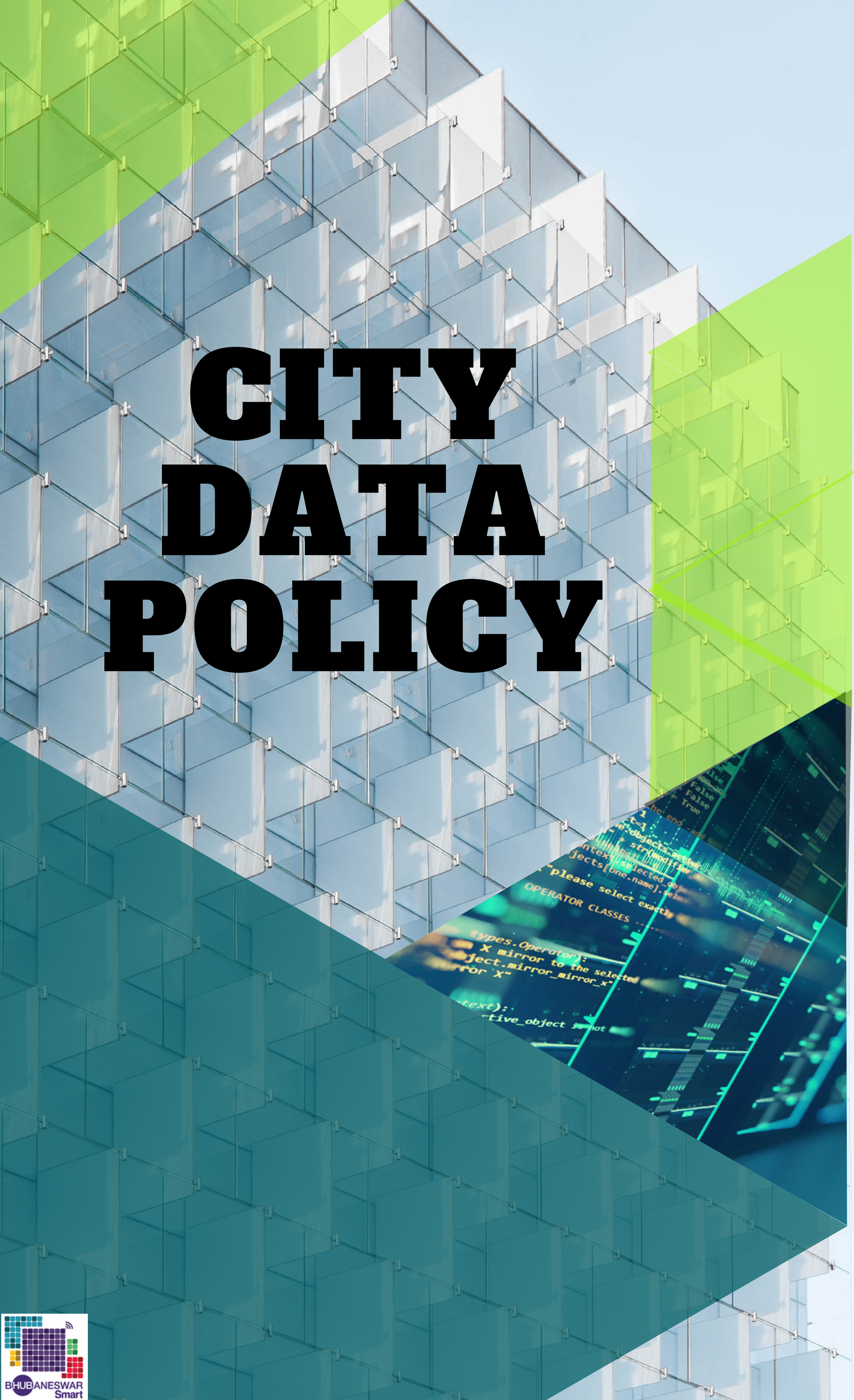
CITY DATA POLICY



BHUBANESWAR Smart

BHUBANESWAR MUNICIPAL CORPORATION BMC

CONTENTS

CONTENTS

1. City Data Policy Checklist

SL NO.	CDP Checklist for Cities	Compliance Status	Reference
1.	Scope of the policy is clearly laid out	✓	Section 1-3
2.	Key stakeholders who will be involved in the process of creating, writing and reviewing the policy are identified	✓	Section 7
3.	The specific components that would form a part of the CDP are identified	✓	-
4.	Information about each component is collected so that all aspects of data are appropriately covered	✓	Section 11
5.	CDP adheres to the principles laid down under NDSAP, DSC Strategy and DMAF	✓	-
6.	CDP includes principles of data classification and categorization, data flow/approval framework, archival and retention policies, and tenets of data security and privacy	✓	Section 12-14
7.	There is adequate information around formation of City Data Team and City Data Alliance	✓	Section 16
8.	There is a clear indication on the access policy of the datasets along with their classification.	✓	Section 9
9.	Ample space is available for data storage, keeping in mind the retention and archival timing.	✓	Section 13
10.	Approvers for various data workflows are defined and intimated.	✓	-
11.	CDP includes pre-defined and agreed upon procedures for data collection, processing and cleaning Responsibilities of various stakeholders are defined	✓	Section 5 and 9
12.	Responsibilities of various stakeholders are defined	✓	Section 7
13.	The policy covers key aspects for its successful and effective implementation including a data governance framework, defining roles and responsibilities of key participants and monitoring policy implementation	✓	Section 16
14.	CDP is reviewed by the identified stakeholders and their inputs have been incorporated	Under Progress	-
15.	CDP is finalized and approved by the relevant authority for public circulation	Under Progress	-

2. Introduction

Bhubaneswar, the capital of Odisha is one of the fastest growing cities of India. The city is an example of perfectly balancing the development and protection of its rich and varied heritage. Bhubaneswar, the temple city was previously known for its rich heritage and culture, of beautiful temples and awe inspiring architectural. The new Bhubaneswar being build by the denizens of Bhubaneswar strongly believes in reaping the benefits of technology. Bhubaneswar has embarked on the journey of digital innovation and data led policy making based on detailed data analysis. Bhubaneswar strongly believes in preempting the threats and providing proactive solutions rather than predictive solutions.

Bhubaneswar had been ranked as the No 1 Smart City by MoHUA based on its smart city proposal. Bhubaneswar envisions to be a

- Transit Oriented City with a compact urban form that promotes active, connected and sustainable mobility choices.
- Livable City – Provides diverse range of housing, educational and recreational opportunities, while enhancing its heritage, arts and traditional communities
- Child Friendly City – Providing accessible, safe, inclusive and vibrant public spaces.
- Eco City – Co-existing n harmony with nature for nurturing a resilient, clean, green and healthy environment.
- Regional Economic Center – Attracting knowledge-based enterprises and sustain able tourism activities by leveraging and empowering its institutions, local business and informal workforce.

Figure 1: Vision of Bhubaneswar Smart City

To move towards a more livable city, the plan focuses on creating a model of sustainable urbanization based on New Urbanism principles. Bhubaneswar's Strategic Plan is built on 5 strategic pillars- Responsive Governance, Transit Oriented Development (TOD) Based Planning and Design, Fiscal Sustainability, Infrastructure and Socio-Economic Development. These pillars are guided by 10 Strategic Directions which are the key strategies for the plan. These together provide the foundation for creating a more inclusive, resource-efficient, and technology enabled future for the city.

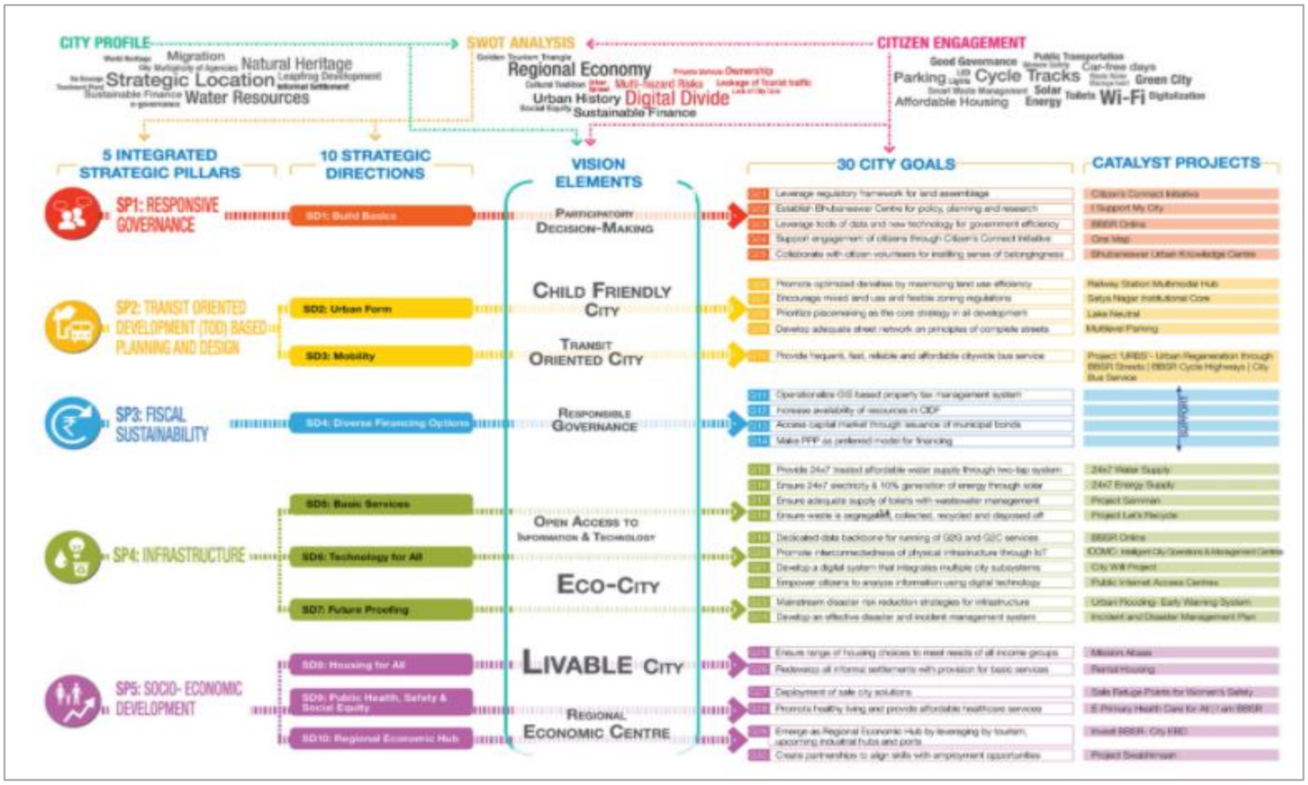

CITY PROFILE
Migration
Natural Heritage
Strategic Location
Leapfrog Development
Informal Settlement
Sustainable Finance
Water Resources
e-governance
SWOT ANALYSIS
Golden Tourism Triangle
Regional Economy
Private Vehicle Ownership
Cultural Tradition
Multi-hazard Risks
Leakage of Tourist traffic
Urban History
Digital Divide
Social Equity
Sustainable Finance
CITIZEN ENGAGEMENT
Good Governance
Public Transportation
Car-free days
Parking
LED Lights
Cycle Tracks
Green City
Smart Waste Management
Solar Energy
Toilets
Wi-Fi
Digitalization
Affordable Housing
5 INTEGRATED STRATEGIC PILLARS
10 STRATEGIC DIRECTIONS
VISION ELEMENTS
30 CITY GOALS
CATALYST PROJECTS
SP1: RESPONSIVE GOVERNANCE
SD1: Build Basics
Participatory Decision-Making
SP2: TRANSIT ORIENTED DEVELOPMENT (TOD) BASED PLANNING AND DESIGN
SD2: Urban Form
Child Friendly City
SD3: Mobility
Transit Oriented City
SP3: FISCAL SUSTAINABILITY
SD4: Diverse Financing Options
Responsible Governance
SP4: INFRASTRUCTURE
SD5: Basic Services
Open Access to Information & Technology
SD6: Technology for All
Eco-City
SD7: Future Proofing
SP5: SOCIO- ECONOMIC DEVELOPMENT
SD8: Housing for All
Livable City
SD9: Public Health, Safety & Social Equity
Regional Economic Centre
SD10: Regional Economic Hub
Leverage regulatory framework for land assemblage
Establish Bhubaneswar Centre for policy, planning and research
Leverage tools of data and new technology for government efficiency
Support engagement of citizens through Citizen's Connect Initiative
Collaborate with citizen volunteers for instilling sense of belongingness
Citizen's Connect Initiative
I Support My City
BBSR Online
One Map
Bhubaneswar Urban Knowledge Centre
Promote optimized densities by maximizing land use efficiency
Encourage mixed land use and flexible zoning regulations
Prioritize placemaking as the core strategy in all development
Develop adequate street network on principles of complete streets
Railway Station Multimodal Hub
Satya Nagar Institutional Core
Lake Neutral
Multilevel Parking
Provide frequent, fast, reliable and affordable citywide bus service
Project 'URBS' - Urban Regeneration through BBSR Streets | BBSR Cycle Highways | City Bus Service
Operationalize GIS based property tax management system
Increase availability of resources in CIDF
Access capital market through issuance of municipal bonds
Make PPP as preferred model for financing
SUPPORT
Provide 24x7 treated affordable water supply through two-tap system
Ensure 24x7 electricity & 10% generation of energy through solar
Ensure adequate supply of toilets with wastewater management
Ensure waste is segregated, collected, recycled and disposed off
24x7 Water Supply
24x7 Energy Supply
Project Samman
Project Let's Recycle
Dedicated data backbone for running of G2G and G2C services
Promote interconnectedness of physical infrastructure through IoT
Develop a digital system that integrates multiple city subsystems
Empower citizens to analyze information using digital technology
BBSR Online
ICOMC: Intelligent City Operations & Management Centre
City Wifi Project
Public Internet Access Centres
Mainstream disaster risk reduction strategies for infrastructure
Develop an effective disaster and incident management system
Urban Flooding- Early Warning System
Incident and Disaster Management Plan
Ensure range of housing choices to meet needs of all income groups
Redevelop all informal settlements with provision for basic services
Mission Abaas
Rental Housing
Deployment of safe city solutions
Promote healthy living and provide affordable healthcare services
Safe Refuge Points for Women's Safety
E-Primary Health Care for All | I am BBSR
Emerge as Regional Economic Hub by leveraging by tourism, upcoming industrial hubs and ports
Create partnerships to align skills with employment opportunities
Invest BBSR: City EBC
Project Swabhiman

Figure 2: Strategic Plan of Bhubaneswar Smart City

As per the Strategy, one of the vision elements identified was Technology for All. Under this strategic vision element, it was identified to empower citizens to analyze information using digital technology. This implied the formulation of a deep-rooted data culture among the city authorities and also of the citizens. In a bid to boost the same, the city data policy for Bhubaneswar is envisaged.

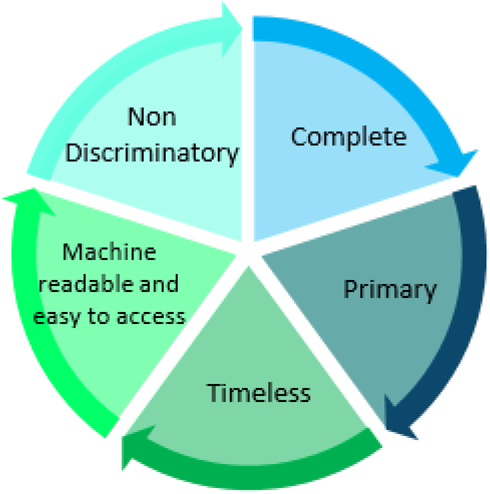
To unlock the power of data in the context of privacy, security and ownership in the context of the city, it is critical that Bhubaneswar creates data policies that balance privacy, legal aspects and public benefit considerations. At the same time, the policy must define the contours of collaboration between various Governmental as well as non-Governmental entities on data sharing and access. Lack of a clear data policy shall be a hindrance to Bhubaneswar from adopting data-driven decision making due to underlying issues such as managing different types of data, data ownership and privacy.

Developing a comprehensive CDP provides clarity on the enterprise processes required to handle data and manage it on open data and exchange portal, helps in identification and segregation of datasets, and introduces accountability by nominating and engaging with departmental data officers. A data policy is also essential to understand the contours of data sharing, standardization, privacy, security and ownership in the context of the city. A CDP is critical to retain the trust between the city administration and its stakeholders, so stakeholders understand that the city data collection exercise is to their long-term benefit.

3. Data as a driver.

Bhubaneswar has embarked on a journey of digital transformation enhancing transparency, accountability and improved service delivery leveraging the benefits of an IoT based environment. Bhubaneswar has a huge data potential based on the number of citizens availing various city services and with the upsurge in digital transactions. The sensor layer used in the field of traffic management, transit management, environmental indices management, a dedicated communication layer, parking management, solid waste management brings in an array of data. These data are used for carrying out regular operations for managing the city indices efficiently. The data has a huge potential and it is envisaged to analyze them efficiently to better predict future of the city and take responsive and data backed policy level decisions. The data also adds a layer of objectivity in clearly highlighting the strengths, weakness, opportunities and threats of the city.

The advantages of data over any conventional method of deciding on the solutions lies in the objectivity of the data, data is non-discriminatory and ensures that all the points pertaining to the situation is well



Covered under the broad aegis of a transparent and high value data sets. The primary principles of a high value data sets are :

- Non-Discriminatory Data:
- Complete Data
- Primary Data
- Timeless Data
- Machine readable and easy to access.

4. As – Is Scenario

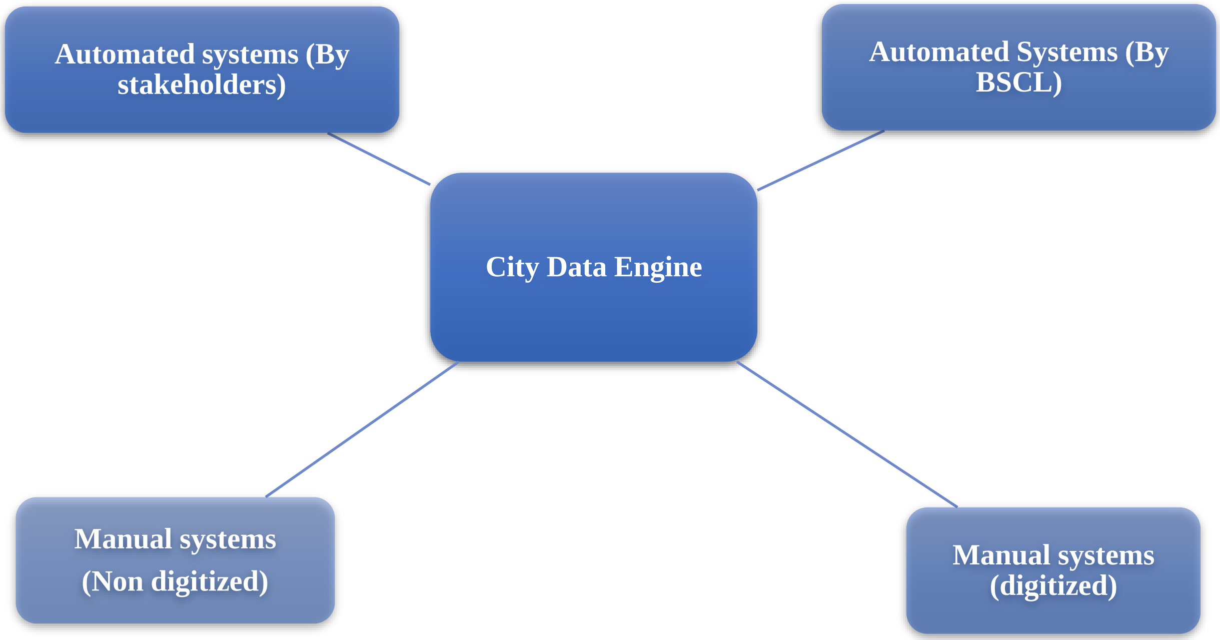
Bhubaneswar presently is undergoing a huge transformation in the digital space. With new technologies induced as part of the Smart City Proposal. The systems can broadly be classified as :

a. **Automated Systems (Ownership of Bhubaneswar Smart City Limited):** These systems have been developed as part of the Smart City Proposal. All source codes and database are the property of BSCL. The data shall be easily available. These data sets will be pre-sanitized and shall be available in the required data format. The system if required, shall provide real time update of data. However, the data management team shall decide on the frequency of data update keeping in view the efficiency of the systems and with a close attention to the storage and archival policies.

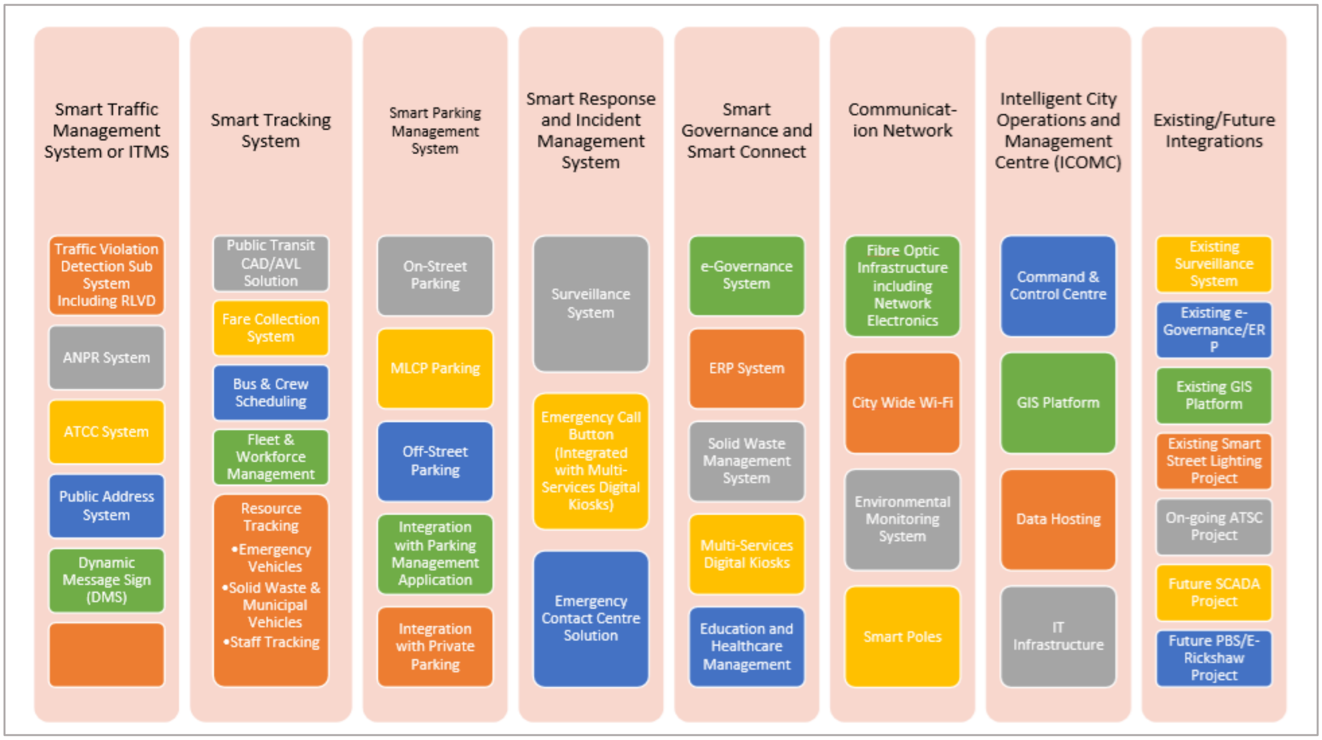
b. **Automated Systems (Ownership by other stakeholders):** These systems have been either existing systems or new systems which have been developed by other organizations not under the scope of Bhubaneswar Smart City Proposal. A detailed understanding of these systems to be carried out and data alliances to be formed with these organizations to ensure API level integration for seamless data communication across the systems.

c. **Manual Systems (Digitized):** These systems are digitized and are maintained in an excel or some other means. However, the systems are not integrated through API. They will be used to integrate these data sets, batch wise to systems.

d. **Manual Systems (Non-Digitized):** These systems are non-digitized and are maintained in hard copies. It is important to understand these data sets and evaluate if the data sets are required. It is important to note if these data sets are real time or static data sets.


Automated systems (By stakeholders)
Automated Systems (By BSCL)
City Data Engine
Manual systems (Non digitized)
Manual systems (digitized)

The broad description of the systems which have been either developed or under the process of development as part of the Smart City Proposal are mentioned below in a pictorial format. The data pertaining to these systems are mostly machine level data. Each of these systems have been briefly elaborated for the readers to have a better contextualization of the data policy framed for the city of Bhubaneswar.



Smart Traffic Management System or ITMS
- Traffic Violation Detection Sub System Including RLVD
- ANPR System
- ATCC System
- Public Address System
- Dynamic Message Sign (DMS)

Smart Tracking System
- Public Transit CAD/AVL Solution
- Fare Collection System
- Bus & Crew Scheduling
- Fleet & Workforce Management
- Resource Tracking •Emergency Vehicles •Solid Waste & Municipal Vehicles •Staff Tracking

Smart Parking Management System
- On-Street Parking
- MLCP Parking
- Off-Street Parking
- Integration with Parking Management Application
- Integration with Private Parking

Smart Response and Incident Management System
- Surveillance System
- Emergency Call Button (Integrated with Multi-Services Digital Kiosks)
- Emergency Contact Centre Solution

Smart Governance and Smart Connect
- e-Governance System
- ERP System
- Solid Waste Management System
- Multi-Services Digital Kiosks
- Education and Healthcare Management

Communicat-ion Network
- Fibre Optic Infrastructure including Network Electronics
- City Wide Wi-Fi
- Environmental Monitoring System
- Smart Poles

Intelligent City Operations and Management Centre (ICOMC)
- Command & Control Centre
- GIS Platform
- Data Hosting
- IT Infrastructure

Existing/Future Integrations
- Existing Surveillance System
- Existing e-Governance/ERP
- Existing GIS Platform
- Existing Smart Street Lighting Project
- On-going ATSC Project
- Future SCADA Project
- Future PBS/E-Rickshaw Project

Figure 3: Proposed Smart City Projects for Bhubaneswar City

A number of automated systems have been developed by different agencies. These systems may also provide real time data which can be integrated with the existing CKC system (Smart City Platforms) as and when the API is made available to enhance the efficiency and accuracy of the data analytics being carried out.

Beyond the automated systems, several organizations in Bhubaneswar still have digital records which are available in excel format. These reports are generated manually, through data entry. A process for batch updation of these data into the system will also be envisaged in the next sections of this document.

The other systems are still maintained in hard copy format. Digitizing these data will be a herculean task and hence, this exercise of identifying the city data assets will further guide the city institutions to automate the legacy system so as to enable a complete digital transformation.

The systems which cannot be integrated at API level, shall be required to share data following a standard operating procedure which shall be agreed upon by the concerned stakeholder organizations.

It is also advised that BSCL being the driver of this data initiative shall form necessary data alliances and MoUs as per the requirement with stakeholder agencies for smooth and seamless sharing of data. The data analysis may also be shared with partner agencies for taking data backed decisions. The detailed Standard operating procedure for the same has been attached in the subsequent sections (Refer Section 23).

5. Objectives of Policy

The broad objective of the policy is:

- Identification of proper data sets.
- Classification of data sets as per the privacy, structure and usability.
- Ensuring the datasets are accurate and latest.
- Efficient storage and archival of data.
- Alignment of all data related operations in line with the national, state and industry wide best practices.
- Enhanced sharing of data among different city agencies using a standard operating procedure.
- Ushering a data culture, where data acts as a prime agent in all planning, implementation and operational activities.
- Setting up a data analysis wire framework for predictive, prescriptive and other analysis.
- Empowering city administrators, agencies and citizens to view, analyze and use data.
- Setting up the cycle of transformation and innovation by providing startups and academicians to analyze data to provide solutions for city problems.
- Clearly setting out the roles and responsibilities of the city data organization structure with clear roles and responsibilities.

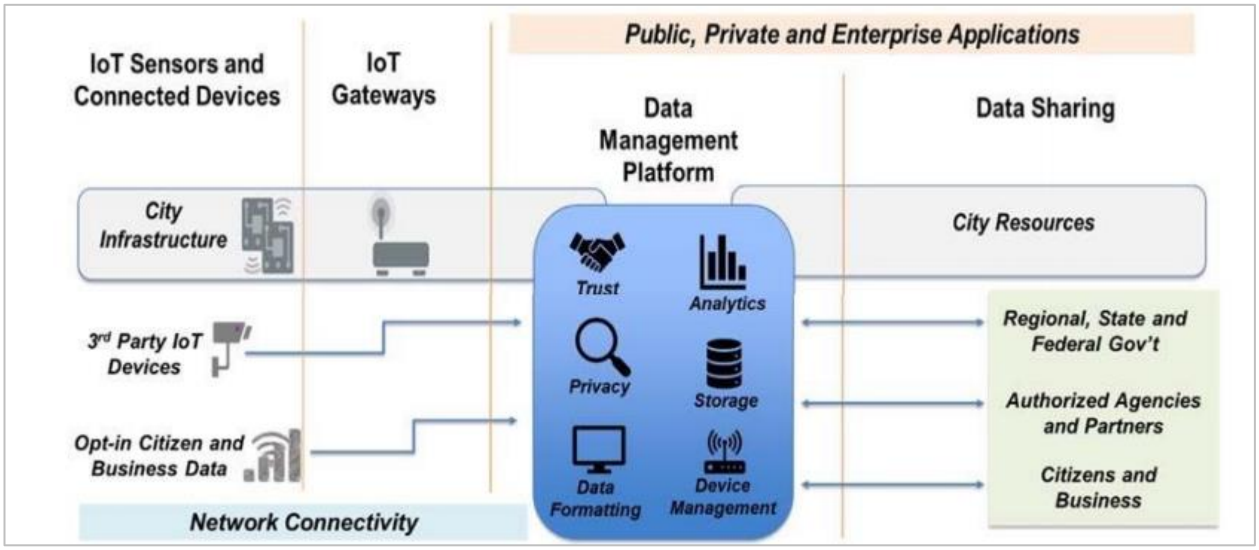


Figure 4: Data can be the foundation on which several cases can be addressed by the city

6. Need of Policy

- Increased Transparency and Accountability thus fostering greater trust on government.
- Increased public participation in government data analysis and deliver solutions or ideas for betterment of city governance
- Improved resource or asset visibility, social audit and open government.
- Better decision making thereby leading to more efficient and cost-effective solutions.
- Deepen open innovation, and co- creation
- Foster data driven decisions by diverse players in urban economic ecosystem
- Foster advanced research in academic and research institution
- Helps cities develop new business models
- Empowers communities through sharing of data promotes development of emerging technologies like AI, ML and Blockchain Enhanced Government to Government(G2G), Government to Business (G2B) and Government to Academia (G2A) collaboration

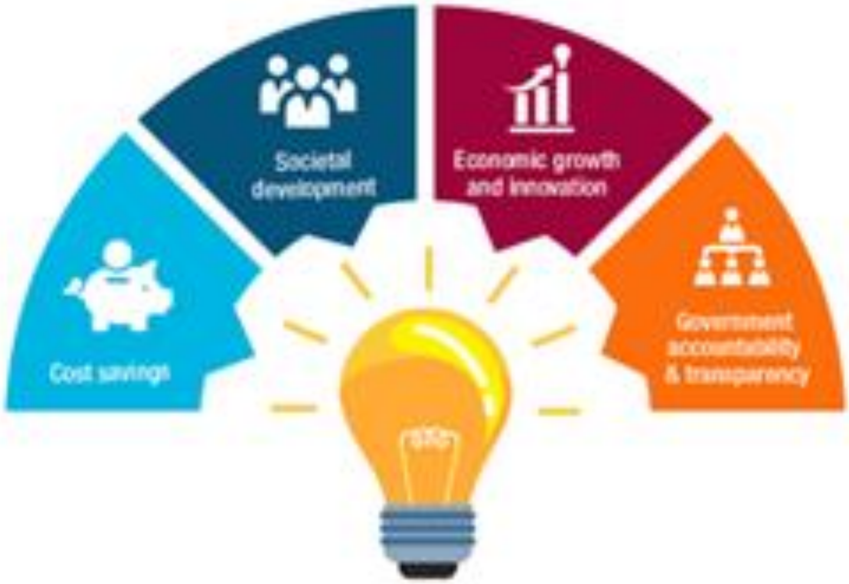

Cost savings
Societal development
Economic growth and innovation
Government accountability & transparency

Figure 5: Benefits of Open Data

7. Gap Assessment

- Currently the city does not have a city data policy.
- Unavailability of a city data team.
- Non-assessment of existing data.
- No alliance between organizations
- No Trust on government data.
- No data audit
- No standard operating procedure for storing, sharing and archiving the data.
- Lack of analysis of data. Data backed policy decisions be taken.

- Non-availability of a city data portal.

8. Stakeholders List

The stakeholder list for the city data policy can be classified as:

- **Organizations for which the systems have been developed:** Certain organizations shall be considered as prime stakeholders. These organizations currently use the system developed as part of the Smart City Proposal. Apart from these systems, the organization might also have certain systems which would be not part of the Smart City Proposal.

The list of stakeholders are :

a) Bhubaneswar Smart City Limited
b) Bhubaneswar Development Authority
c) Bhubaneswar Municipal Corporations.
d) Capital Region Urban Transport.
e) Bhubaneswar- Cuttack Police Commissionerate

- **Organizations which shall be providing data through their systems or manually**. These organizations don’t have any system developed as part of the Smart City Proposal. These agencies/ organizations have huge amount of data which is necessary for efficient analysis and these data sets are vital for publishing to the citizens.

  The tentative list of stakeholders are:

a) Transport Department.
b) Water Department.
c) Forest Department

- **Organizations which would be using the data sets through the city portal**: These organizations don't generally have any system from which data shall be shared. It is rather, that these organizations would be the major beneficiary of the data sets and of the analysis which is done. These organizations shall use the data and do necessary data analytics. Some of the tentative list of organizations which can be listed in the category are as mentioned below:

a) Planning Institutions
b) Central Department Institutions
c) Academic Institutions
d) Non-Governmental Organizations
e) Citizens
f) Funding Agencies
g) Startups and Incubators

- **Guidelines for engaging Stakeholders**

There should be a well-defined process for engaging stakeholders to assess the data needs of the City. CDOs along with the team of Data Champions/Coordinators must assess the data requirements of various stakeholders in smart city. Stakeholders can be engaged by using the following methods:

a) CDO to identify three to four critical areas for the city and examine the system to identify the real issues city is trying to solve and to understand the relationships in the system
b) Based on the dimensions of domain knowledge, influence, public outreach, financial leverage, mandate and incentives, CDO to identify the types of partnerships required
c) CDO to have a roadmap on the critical areas for data collaboration including mission, vision, time, cost, risks and scope
d) CDO to ensure effective implementation of the partnership with appropriate documentation, key performance indicators and deliverables
e) CDO needs to mobilize action from different stakeholders with different roles and power, co-define the process, co-develop solutions, and co-deliver actions and adopt an incremental, problem-driven, iterative approach that promotes experimentation, innovation and learning
f) CDO to enable outreach via communities such as co-working spaces, developer groups through mechanisms such as data meets, hackathons, developer communities etc.

9. Categorization of Data

a. Data Categorization

Data will be categorized into two broad categories:

9.1.1 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.

Note: Personal Identifiable Information cannot be published by City on Data platform under any data sets. Data sets must be anonymized before publishing.

9.1.2. 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.

10. Types of Classification

The classification of data is based on certain parameters which has been defined below:

10.1. Based on generation of data.

Class	Definition
Sensor generated data	This data is generated from on-field sensors.
Manually generated data	This data is generated based on data entry of forms. This form can be filled either by the citizens, officers or by enforcement agencies.
Derived Data	This data sets are derived data and are based on the running of algorithms considering both sensors generated data and manually entered data.

10.2. Based on frequency of generation of data.

Class	Definition
Real Time Generation of Data	These types of data are generated in real time and these are fetched and displayed from the systems in real time. This data sets do not require any authentication and validation as these are data generated from running applications.
Batch Processing of Data	Certain data sets are processed in batch mode to conserve battery backup of the

	field sensors. This data is not shared in real time onto the server but rather shared in batches.
Static data	This dataset are not changing regularly. This type of datasets is dependent on periodic surveys and the frequency of this data sets is to be pre-fixed.

10.3. Based on security of data.

Class	Definition
Public	Data available for public consumption and use.
Internal Use	Information which could only be disclosed to BMC/BSCL employees for managing operations or delivery of public services on day to day basis.
Sensitive	Sensitive data as defined in various Acts and rules of the Government of India.
Protected	Protected for e.g. Identity of citizens and disclosure /notification needs to be issued by BMC/BSCL in case of any breach or loss of data
Restricted	Data which could lead to threat to life or loss of public assets or critical infrastructure.

11. Process of Classifying data – Checklist

- Data collected from other organizations will already have been classified based on the publishing permission.
- In case, the data are not classified, the same shall be requested from the department. If the department, is not providing the classification of data. The data committee shall classify the data.
- Machine Generated Data shall be classified by the system owning agencies.
- The classification of data is mandatory, any data which is not classified shall not be available for sharing and consumption.
- The classification of data shall be in line with the state and nation data policy, aligning with the Open Data Policy and ISO norms.

12. Identification of data sets

- Focus on identifying high value datasets that would have direct impact on citizen welfare will (in terms of city infrastructure and services) and the overall wellbeing of citizens. Based on the utility of these data sets, the city data authority could substantiate cases for garnering additional technical support and funding from state and central government.
- This set can serve two purposes - as a primary set of datasets to begin the initiative (basic datasets), or as a reference set of datasets which BMC/BSCL should consider keeping adding datasets (Intermediate or Advanced datasets) to the Open Data portal.
- Demand of Public Data Sets Like any other product or service offering, demand of the data set should be one of the key drivers while deciding about making it public. Key focus groups influencing this demand should be identified and engaged with during at an early stage for their inputs on particular datasets and. the priority with which it is required. In some cases, data authority could present a list of datasets that can ask the focus group on data that would meet Public need.
- Social Impact - Datasets which potentially could create a positive social impact, irrespective of the economic value generated, should be included. Such positive impacts can include generation of employment, boosting equality and equal opportunities among citizens, address social issues like improving female student enrolment in primary and secondary schools, and empowerment of the backward or oppressed classes etc.
- Economic Value Generation - Publishing certain datasets can boost innovation, encourage entrepreneurship eventually resulting in generation of economic value. Greater economic value could have a far-reaching impact - including generation of employment, boosting per capita income, and bringing overall prosperity for the city and the nation. Data authority should identify and prioritizes Open list datasets into ‘high value' datasets and 'non-high' values datasets on basis of dataset's potential to generate economic value.
- Legal and Compliance requirement There can be legal and compliance requirements for mandatory disclosure of a certain dataset to the public. Data authority should proactively identify datasets, publishing which would help reduce volume' of RTI queries significantly, and could result in lowered burden on city authorities.
- Minimal Resistance - Opening up data sets can have huge implications politically as it could potentially unearth issues and problems that could take a political angle. ': once the data is made public. City Authorities need to be conscious on how data represented and made accessible, so it can be utilized by various parties.

13. Collection of data

The data can be collected through three broad methods:

13.1. API Level Integration: Data which shall be collected from existing systems shall be done based on API Level integration. This shall ensure that the data collection process is completely automated. The steps for ensuring the collection of data through this method shall entail several key considerations.

The Data authority shall define the types of data which shall be required from the system. This shall be a comprehensive list of data points. The data sets once finalized can not be modified easily and modification at API level shall be required to fetch new data from the system.

Ideally, it is suggested that for 3rd party integrations the data sets be pre-defined and the process for adding any additional data sets shall be approved through a data authority.

The APIs once finalized shall be shared and the sample testing shall be done of the data. Once, the data have been received successfully the same shall be placed into the production environment.

The APIs shall be documented and finalized.

13.2. Excel based Upload Mechanism: Certain datasets which shall be required from other departments as identified by the city data authority may not have a system. In, this case it is suggested that excel format of the data be shared.

The template for the same may be shared by Bhubaneswar Smart City Limited and can be available in the city data dashboard, which can be downloaded and submitted. In case, the same is not provisioned for the agency shall share the data on the identified mail id or can be placed in a shareable Google sheet.

It is pertinent to note that to ensure accountability of the other agencies/ organizations, the points shall be delved in the data alliances MoU which shall be signed between different city agencies and organizations.

13.3. Hard Copy of data sets: As part of automating the entire process of data analysis it is important to identify data sets which are available in hard copy. Hard copy data sets which shall be submitted through mail and can be handed in person. A frequency of submission of these data sets shall be mutually agreed by the stakeholders and by BMC & BSCL.

14. Quality Assessment of Data

Overall, the whole process of quality assessment of Data enables to evaluate the city data scientifically and statistically to determine whether they meet the quality required for the project and are of the right type and quantity to be able to support the need of the project. These are a set of guidelines and techniques that are used to describe data, type of data, and to apply processed to assess and improve the quality of data. The quality assessment allows the organization to properly plan for data cleansing and enrichment strategies. This is carried out to maintain the integrity of city systems, quality assurance standards, and compliance concerns. Usually, quality issues such as inconsistent structure and standard issues, missing data or missing default data, and errors in the data fields are easy to detect and verify with the help of quality assessment. It has five dimensions of data quality that are, accuracy and reliability, serviceability, accessibility, methodological soundness and assurances of integrity.

The quality of data can be accessed through five broad steps:

14.1. Defining the project goal

Defining the city project goal for data quality improvement, stakeholders, the impact business processed and city data rules which ensure all the records made are unique, information is accurate, and the data is consistent across multiple systems.

14.2. Data assessment

This step involves assessing the data against multiple dimensions such as consistency of attributes across multiple data sets and timeliness of data. Depending upon the volume and variety of data assessment will be done in terms of qualitative and quantitative assessment using profiling tools. This is the step where the existing policies are assessed which includes data access, data security, adherence to compliance guidelines.

14.3. Data Analysis

This step involves analyzing the assessed data to analyze the gap between project goal and current data. It also helps in measuring the inconsistency of the accessed data.

14.4. Data Improvement

This step involves designing and developing improvement plans based on the preceding analysis. The plans made would consist of comprehend timeframes, resources and the cost involved.

14.5. Implementation

The implementation stage is determined in the data improvement stage. This step involves comprehending both technical as well as project process related changes.

14.6. Interpretation of results

Verification of data at periodic intervals that the data is consistent with the project goals and the data rules specified in the first step (Section 1.1.). This step involves communicating the data quality metrics and current status to all stakeholders on a systematic basis to ensure that data quality is maintained on an ongoing basis across the departments.

15. Storage of Data

Determining the best data storage method is the most important factor for the organization because these data are much more essential than mere information. These data stored are assets for the project to make major decisions, utilizing powerful algorithms to derive valuable insights from the structured data. Storage of data can be done on premises or off premises and various cloud-based options.

Three types of data storage are categorized below:

15.1. Cloud Storage

Cloud storage is offsite computing of data that can be accessed anytime, anywhere by the organization. This storage method is preferable because of benefits like flexibility to increase or reduce costs and storage as needed and the organization doesn’t have to worry about the maintenance.

15.2. Server Based (Hyper Convergence)

Server based, or hyper convergence storage allows the data to be stored within the individual server at the data center i.e. on the site/ department. This storage method is preferable because of benefits like fast and cost-effective way to escape an overcomplicated structure of a data structure that would have been created over time.

15.3. Traditional Storage Systems

Traditional storage is used as a backup method for the cloud. For security reasons, it can be usually only be accessed while signed into the internet connection. This storage method is preferable because of benefits like affordability, faster data access time and scalability.

16. Data Archival

Data archival is the intentional preservation of data in a specific format made by the organization that makes it easy for stakeholders to refer to the data whenever required. Archival of data is used to save and store the changing data, recover, and restore lost files/ data. This method is used for storing static data that cannot be changed once it gets recorded in the organizational database. This method is preferable as it reduces primary storage and allows the department to maintain data that may be required for regulatory requirements.

The data archiving process usually uses automated software, which will automatically move “cold (i.e. archived)” data via policies set by the administrator. Data archiving can take several different forms. The options can be online data storage, which places archive data onto disk systems where it is readily accessible by the users. Another archival system uses offline data storage where data is stored in any removable media rather than keeping it online. The last option for data archival is using cloud storage.

16.1. Data Backup Guidelines

Data backup or retention is the effect of copying or archiving files and data for being able to restore them in case of project data loss as it can be caused by many things starting from computer viruses to hardware failures to file corruption to fire to flood etc.

Steps to find out the best backup strategies:

16.1.1.Hardware Backup Policy

The hardware backup is installed on site in the project location which comes with a storage component. The major benefit of hard drives is that it can be simply attached to the local project network.

16.1.2. Software solutions

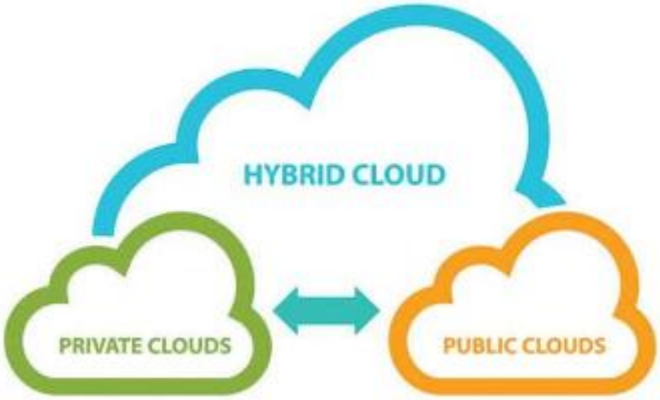
Software solutions are more preferable because these are less expensive than the hardware options. Software solutions can be effortlessly installed on the system which may not need a separate server for it. It is mostly installed on a virtual machine/ mechanism. This can be the best choice if there is a lot of change in the project infrastructure.

16.1.3. Cloud Services

Cloud backup services offer offsite backup of data. These services allow to run backup and store it in the vendor's cloud infrastructure. City projects are mostly data sensitive therefore the major benefit of choosing this backup method is that it is affordable and secure.

16.1.4. Hybrid Solutions

Hybrid Solutions combine software and cloud backups to provide multiple options for restoring data. It has two benefits if installed by the organization i.e. there will be on site backups along with cloud-based backup whenever necessary.



17. Analysis of data

Smart cities are built on digitized data, which is increasingly derived from the Internet of Things (IoT). As storehouses of digital data grow, many cities and businesses have recognized the need to analyze this data in an efficient way.

Apart from presenting the actual data, cleaned datasets might also be used to discover new patterns or analyze existing patterns, trends or behaviors. Data analysis may help multi-disciplinary researchers provide different perspectives or even solutions on civic issues like transport, traffic, solid waste etc.

Data analysis comprises of tools and methods used to process structured and unstructured data on various dimensions for various purposes. Analysis of data could be carried on under 6 major ways:

17.1. Define your Questions:

This is the first step where questions are designed to either qualify or disqualify potential solutions to specific problem or opportunity. It should be measurable, clear and concise. Null and alternative hypothesis are being formed and the analysis of the entire research revolves around the same.

17.2. Set Clear Measurement Priorities:

The scale of measurement is decided from the below listed categories:

- Nominal Scale: non-numeric categories that cannot be ranked or compared quantitatively. Variables are exclusive and exhaustive.
- Ordinal Scale: exclusive categories that are exclusive and exhaustive but with a logical order. Quality ratings and agreement ratings are examples of ordinal scales (i.e., good, very good, fair, etc., OR agree, strongly agree, disagree, etc.).
- Interval: a measurement scale where data is grouped into categories with orderly and equal distances between the categories. There is always an arbitrary zero point.
- Ratio: contains features of all three.

17.3. Collect Data-

This step involves collection of data either from primary or secondary sources i.e. in the form of API Level integration, excel based upon mechanism and hard copy data sets.

17.4. Analyze Data-

In this step, data is manipulated in several ways and correlation is found in excel. This lets to filter out similar variables and enables sorting of data. Mean, median, mode and standard deviation of the dataset is being calculated under this step. The main methods of data analysis are as follows:

- **Descriptive Analysis**: Descriptive Analysis considers the historical data, Key Performance Indicators, and describes the performance based on a chosen benchmark. It considers past trends and how they might influence future performance.
- **Dispersion Analysis**: Dispersion in the area onto which a data set is spread. This technique allows data analysts to determine the variability of the factors under study.
- **Regression Analysis**: This technique works by modeling the relationship between a dependent variable and one or more independent variables. A regression model can be linear, multiple, logistic, ridge, non-linear, life data, and more.
- **Factor Analysis**: This technique helps to determine if there exists any relationship between a set of variables. In this process, it reveals other factors or variables that describe the

patterns in the relationship among the original variables. Factor Analysis leaps forward into useful clustering and classification procedures.

- **Discriminant Analysis**: It is a classification technique in data mining. It identifies the different points on different groups based on variable measurements. In simple terms, it identifies what makes two groups different from one another; this helps to identify new items.
- **Time Series Analysis**: In this kind of analysis, measurements are spanned across time, which gives us a collection of organized data known as time-series.

These analysis are inherent to the smart city platform and shall be fetched from the smart city platform and showcased in the Open Data City Portal.

17.5. Data Visualization-

Data Visualization involves deriving valuable insights by comparison of datasets and observe relationships. This step involves graphical representation of the analyzed data sets and to use color, size, scale, shapes and labels to attract attention to key messages.

The data visualizations shall be taken up through the central data portal. The data portal shall act as a platform for carrying out all analyses mentioned above with relevant visualization which can be changed by the users on the go as per the requirement.

18. Sharing and Publishing of data

The data which has been collected by the various stakeholder agencies shall need to be published as part of the Open Data Policy. The data shall be made available to the different stakeholders, as per the requirements of the different agencies and based on the access restriction of data.

Bhubaneswar Smart City Limited in collaboration with Bhubaneswar Municipal Corporation shall be developing a city level data dashboard which shall ensure that the data directories available for public consumption are available for download. These data sets can be previewed and downloaded in the various formats.

Beyond the same, there would be certain data sets which shall not be classified as data and shall be restricted based on the accessibility of data. A data portal will allow the agencies and citizens to place their request for the data which are not classified as open data. However, in the interest and in support of open data, the data portal shall provide a simple data directory which shall list the data available, along with its key attributes as data restriction, last update date, number of data-sets available and the agency contributing these data sets. A detailed record of the people accessing the non-open data shall be recorded.

The data authority shall play a vital role in defining the guidelines and detailed SOP for sharing the datasets apart from the open source data.

Certain government agencies shall be provided access to data sets which shall be agreed upon during the city data alliance and partnership stage with different city agencies. A credential shall be provided to the identified agencies and the data shall be made available to them in a downloadable form.

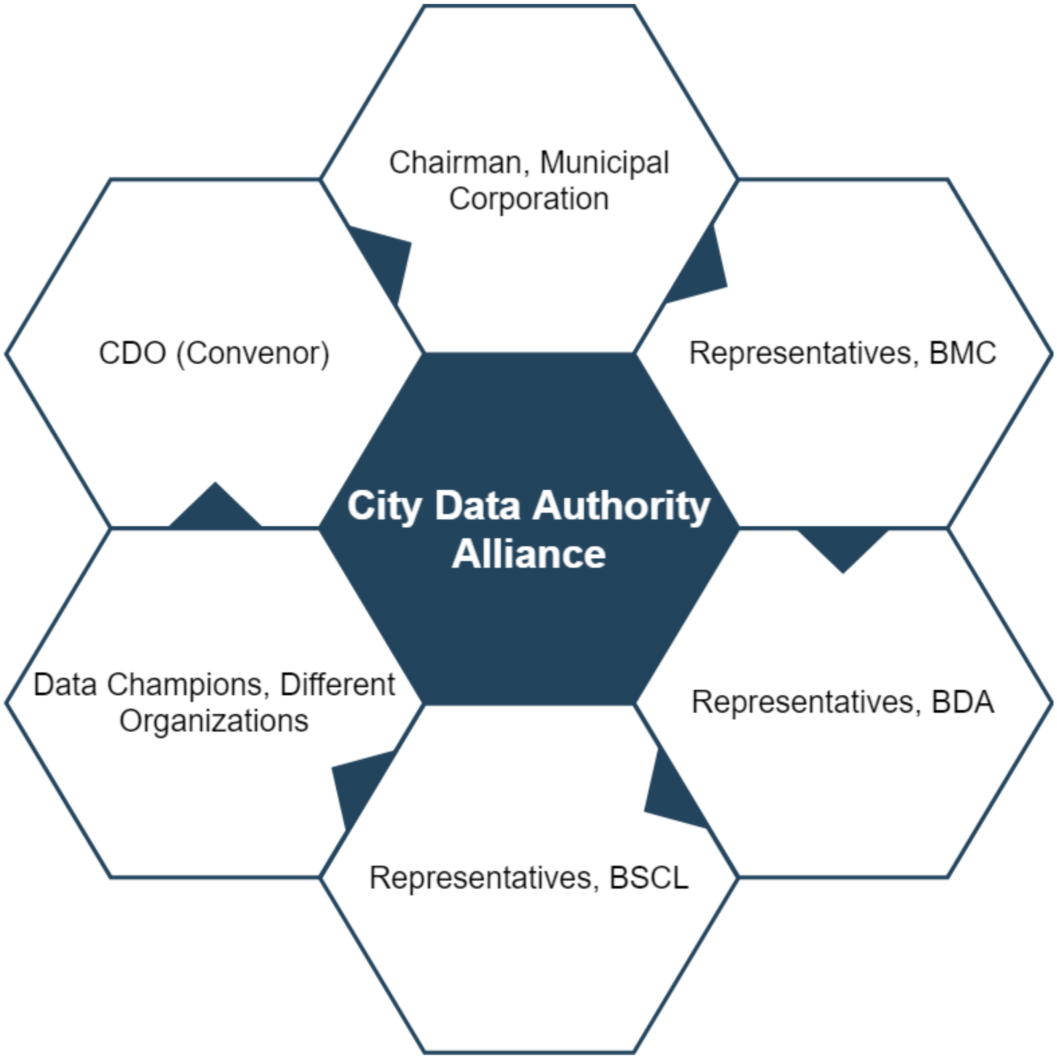
The data shall also be made available as an API integration platform. All data sets shall be made available as an API also for all the data platforms. The API can be made available on request. This shall be taken up eventually.

19. Data Organization Structure - Responsibility Matrix

A City Data Committee should be made to seek participation and secure buy in from both internal and external stakeholders and collaborators on key decisions. Additionally, sufficient empowerment of this committee will help to navigate complicated hurdles which may include bureaucratic and political obstacles and to promote decisions and action pertaining to collection, release and segregation of open data.

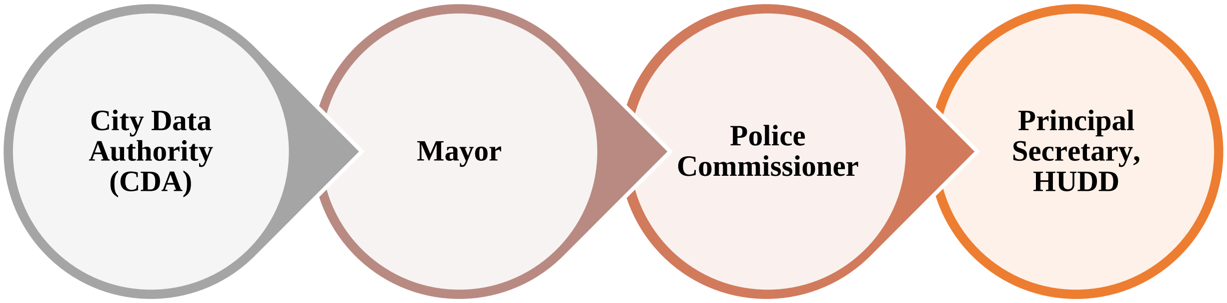
19.1. City Data Authority Alliance

- Key function: Reviewing
- Meeting Frequency: Monthly


Chairman, Municipal Corporation
CDO (Convenor)
Representatives, BMC
City Data Authority Alliance
Data Champions, Different Organizations
Representatives, BDA
Representatives, BSCL

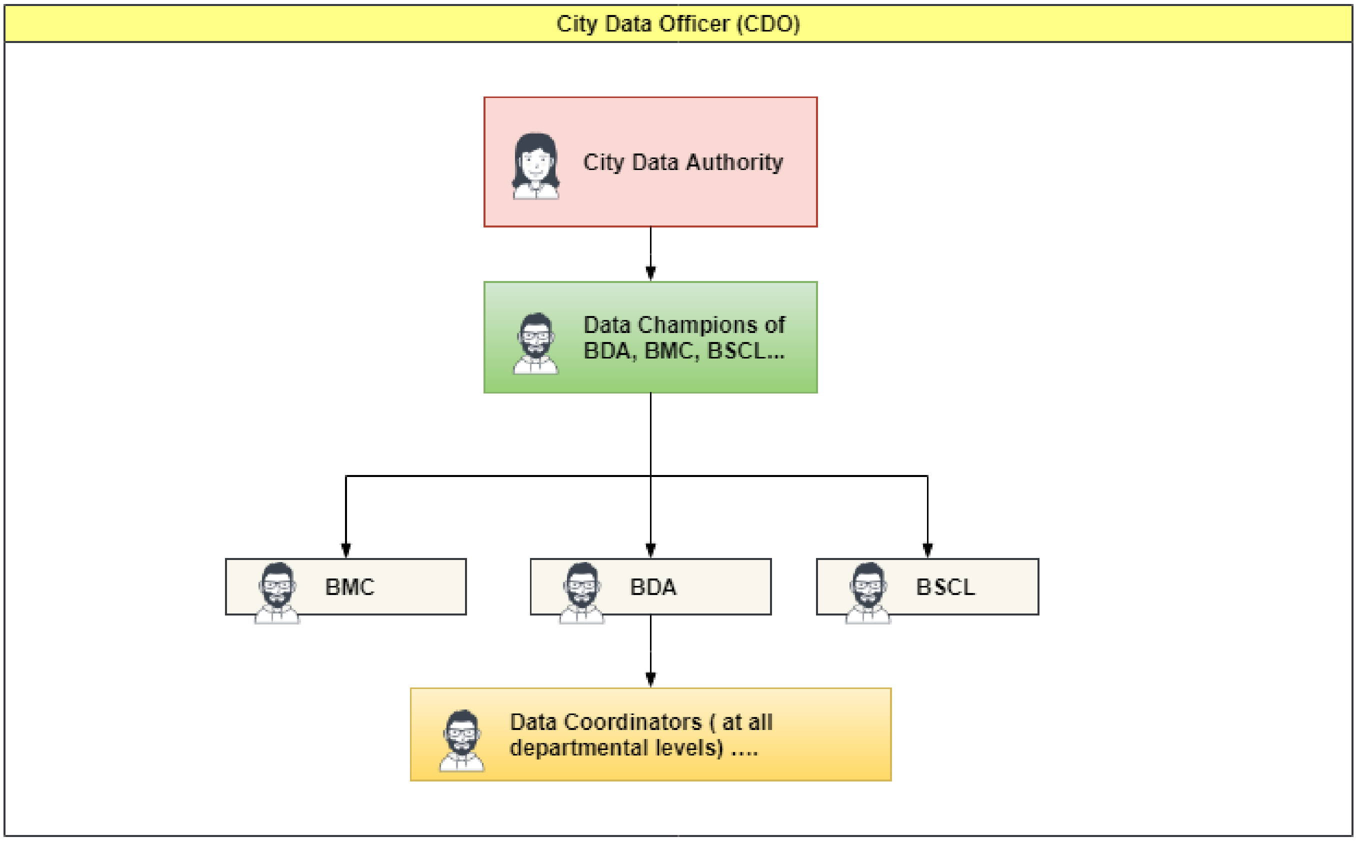
19.2. Standing Committee

- Key function: Ratification
- Meeting Frequency: 6 Months



19.3. Organizational Structure

Each organization will have to identify the person and the same will be shared in the matrix.


City Data Officer (CDO)
City Data Authority
Data Champions of BDA, BMC, BSCL...
BMC
BDA
BSCL
Data Coordinators (at all departmental levels) ....

19.4. Roles and Responsibilities

19.4.1. City Data Officer (CDO)

The CDO is the person responsible for implementation of this data strategy at the city level. The key responsibilities of the CDO officer are as follows:

- The CDO will form City Data Policy (CDP) which has to be reviewed every month to keep it contextual as per the need. The CDA will act as advisory body for the review of CDP from time to time.
- Coordination with MDO (Mission Data officer) to align with mission data strategy and priorities with respect to Open government initiatives and policies.
- Organizing regular meetings of the City Data Alliance (CDA)
- Coordinate with officers of various other government departments/agencies/stakeholders within the city for the effective implementation of City Data policy.
- Publish Data Catalogues and Data Sets/Feeds on OGD portal: CDO will publish data Catalogues and Data Sets/Feeds on OGD Portal and ensure that data sets are updated at regular time intervals as needed and create mechanism for continuous feedback from citizens and stakeholders on type of data sets to be published and released

19.4.2.Data Champions

Data Champions will be of senior-level functionaries, who will not be below the rank of a Head of Department or equivalent, who would champion the implementation of the CDP in the respective project or departments. Active participation from data agencies will be key to the successful collaboration of data within the city. Data champions will be the flag bearers of the policy in the whole duration of the project being implemented or for the respective organization and would work to align in their teams to imbibe the principles of data driven decision making on a day-to-day basis. Major roles and responsibilities to be performed by data champions are as follows:

- Data Champions (DCs) to identify the data sets, derived information, intelligence or data challenge as per to day to day operations of the department.
- DCs to actively publish or enable to publish data sets/feeds identified relevant to the resolution of critical cases for the city. DCs will work closely with the CDO for active implementation of the City Data Policy.
- DCs will be assisted by the Data Coordinators (DCOs) within the department to streamline processes of data reporting, collection and analysis of data. Data Champions will be responsible for the data quality.
- DCs to undertake activities to engage with the stakeholders and evolve their department's strategy on data in line with the deliberations.
- DCs needs to act as trainers and lead the team of data coordinators at the department level
- DC are the nodal point for implementation of the CDO within the department and will function to supervise the team of data coordinators on a daily basis.
- DC are the first touch point of CDO in different organizations in the city and must undertake continuous capacity building programs for their respective DCOs and other staff.

19.4.3.Data Coordinators

- Data Coordinators to assist Data Champions at the department/government Level as reporting staff.
- Data Coordinators to aggregate the data demand from various channels
- Data Coordinators are responsible for sensitizing the department employees over the importance of data quality
- Data Coordinators to perform collection, interpretation and recording of data in accordance with City Data Policy standards and CDO guidelines
- Data Coordinators to perform data validation and storage of various project documents
- Data Coordinators to review required data and documents & make necessary revisions for the same
- Data coordinators to sort and organize the data both in hard copy and soft copies
- Transmit data report to BMC/BSCL or CDO via Internet (E-mail)
- Update BMC/BSCL website or Bhubaneswar Open Data Portal with latest data records
- Data Coordinators to maintain the completed hard copy and electronic files of project records
- Data Coordinators to assist department staff in data entry whenever required
- Data Coordinators to provide data management updates in all internal and external meetings as required
- Data Coordinators to analyze data for quality improvement purposes
- Data Coordinators to prepare data for reporting, meeting and presentations for their department and BMC / BSCL at large
- Data Coordinators to ensure data management procedures to comply with the City Data policy
- Data Coordinators to provide statistical analysis and longitudinal analysis of data
- Data Coordinators to prepare and submit data required for audits

19.4.4.City Data Alliance (CDA)

CDA is envisaged for the city to be the network of government departments, agencies, private sector companies, community organizations, domain & legal experts, city policy makers, researchers, academic institutions, incubators, entrepreneurs within the city who come together voluntarily as a collective to diagnose the problems in the city problems which need resolution, act as an advocacy group for the formulation of the CDP which defines the collective approach of the city issues relevant to the data. The key roles of CDA are as follows:

- CDA to act as an advisory group to the city leadership on the City Data policy
- CDA to promote data driven governance and policy formulation
- CDA to design and implement solutions and analysis using city data
- CDA to support industry to design solutions using emerging technologies like AI, ML and Blockchain.
- CDA to assess and design use cases critical to the citizens of the city.
- CDA to generate awareness in various stakeholders towards open government initiatives.

- CDA to facilitate data for co-creation and collaboration over civic issues
- CDA to provide critical feedback to the city over the quality and relevance of data provided by City.
- CDA to design and develop prototypes/ solutions annually on Civic Problems the City
- CDA to organize a data, challenge every half yearly on complex civic problems
- CDA to organize a Hackathon annually and support shortlisted solutions at city level
- CDA to set up scholarship for postgraduate and graduate interns to work with Office of CDO (optional).
- CDA to publish the progress report every month
- CDA to prioritize the Data Sets/Feeds for publishing on Data platform
- CDA to sensitize ecosystem partners to share the data for leveraging data for solving civic challenges
- CDA to support, engage and encourage network/groups/members of data enthusiasts in the city
- CDA to improve city capacity over data driven governance and policy formulation.
- CDA to support CDO by extending resources (like interns, researchers, technology experts), funds (program sponsorship etc.) and technology (solutions etc.)
- CDA to share data available with partners on Data Platform to promote City Data

20. ISO Norms

The city data policy is enacted as per ISO 27701 and ISO 27001. (Refer Annexure A)

ISO norms are a set of rules enacted by the organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. Characteristics of quality security policies which include conciseness, readability, actionability, enforceability, and flexibility. Policies are short and to the point in conveying principles that guide activity within the organization. Policies contain a minimum of specialized vernacular and acronyms; clearly explain any project-specific terms. The policy must allow for determination of compliance with the policy and enforcement of noncompliance. In addition, policies should potentially apply to the organization for years and not become outdated with the end of life of any project supporting the policy. Any mention of specific product use is in a standard, not a policy.

21. Other Items that may be included

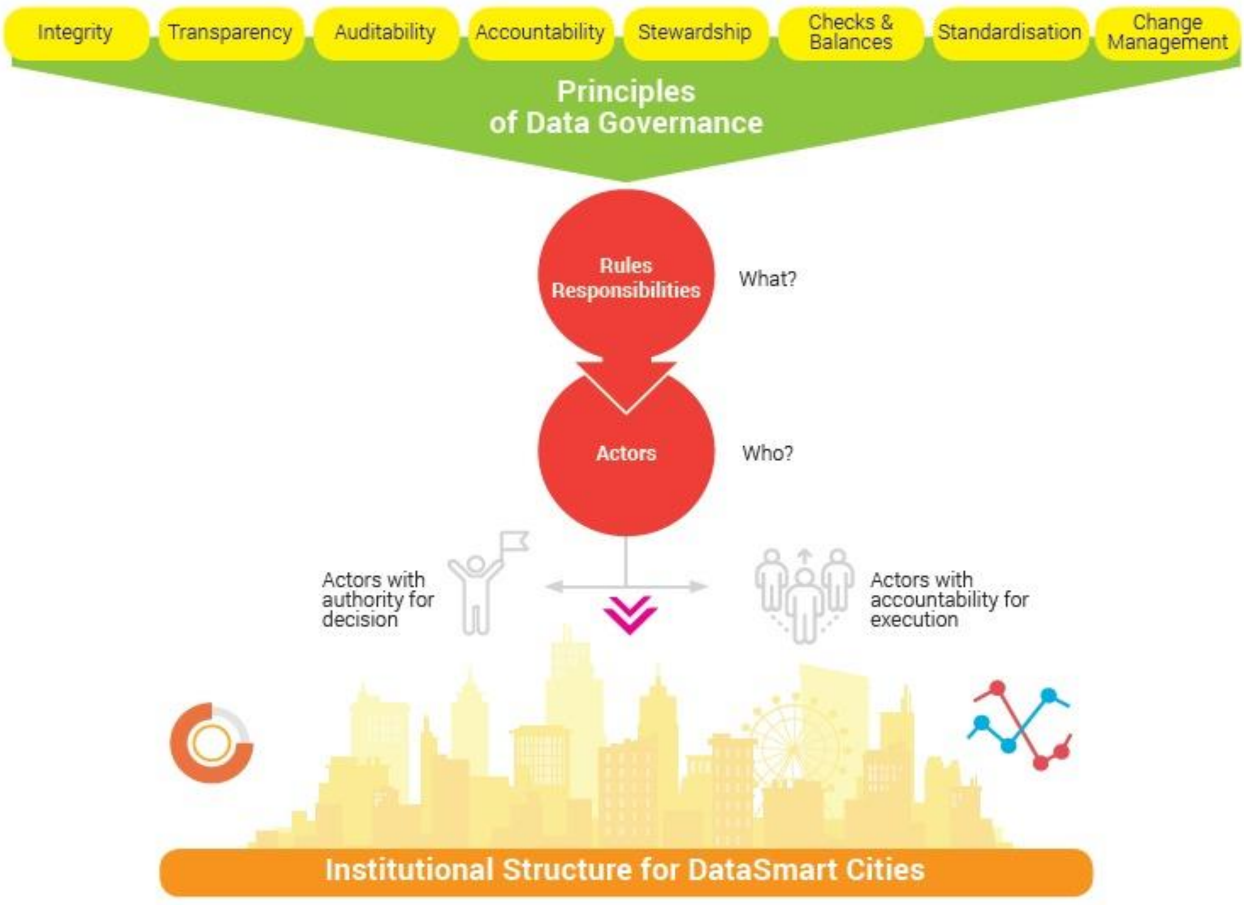
- Virus Protection Procedure
- Intrusion Detection Procedure
- Remote Work Procedure, Technical Guidelines
- Audit
- Employee Requirements
- Consequences for Non-compliance
- Disciplinary Actions
- Terminated Employees
- Physical Security of IT
- References to Supporting Documents

22. Partnership on Data

Opening public data for reprocess or reuse is associated with many advantages, which includes positive impact on the overall issues of the city. This form of partnership includes data sharing and collaboration which can also be known as collaborative goal formed by the government from different projects/ department.

Major benefits of partnership of data includes the following:

- New forms of partnership outside the organization emerge to leverage the explosion of data for public and overall city good.
- Datafication is the catalyst for forming new partnerships.
- It helps in bridging the gap in expertise and knowledge required for city development and for city good.
- The information flow will be huge in terms of inter and intra organizational structure.
- It acts as a tool for analyzing performance for another department


Integrity
Transparency
Auditability
Accountability
Stewardship
Checks & Balances
Standardisation
Change Management
Principles of Data Governance
Rules Responsibilities
What?
Actors
Who?
Actors with authority for decision
Actors with accountability for execution
Institutional Structure for DataSmart Cities

23. Compliance to existing national and state data policy

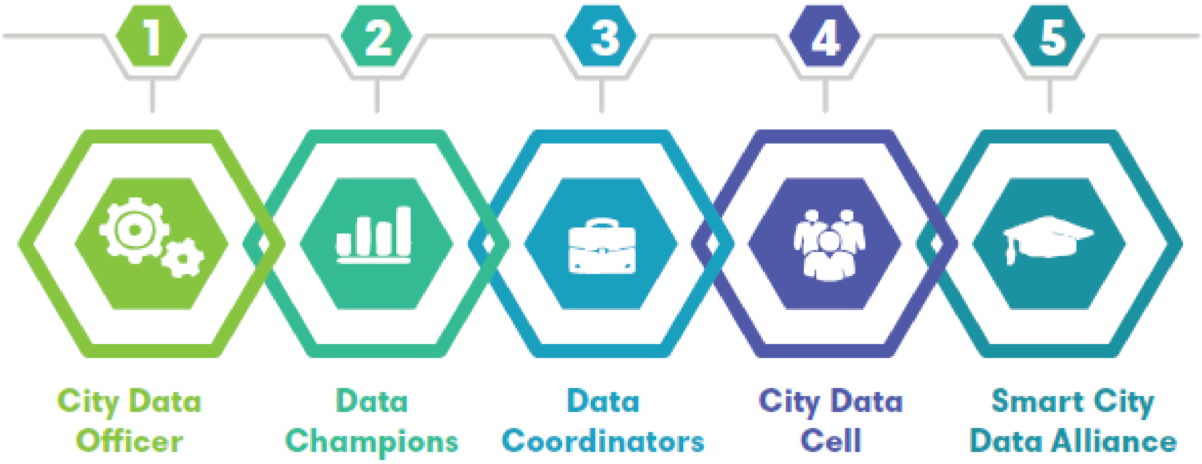
- City data policy is made to as per national data policy i.e. The Information Technology Act, 2000 (IT Act) i.e. SPDI Rules
- It is also made as per the state data policy i.e. Odisha Data Center Policy, 2020

(Refer Annexure B)

24. Policy Implementation and Governance

Creating the policy solves one part of the system but effective implementation is the rest. The City needs to ensure the CDP is implemented as per the guidelines. A central mechanism should be defined to monitor the implementation and other related activities of the policy at the city level at regular intervals. There it needs to be defined roles and responsibilities for the key stakeholders and those driving the policy at the city level. Also, there needs to be cohesiveness among such frameworks being implemented at the national and state levels. DSC Strategy can also be referred for more details. Below are some key aspects that should be kept in mind while designing the CDP:

- **Data Governance:** Only having the data is not enough, it should be reliable, trusted and in a form, which can be utilized in future. This leads to the need of a Data Governance Framework, which will define the decision-making process and authority for data-related matters. Incorporating accountability measures such as reporting requirements will strengthen data governance within the city. These may include creating public registries of all data sharing agreements and data exchanges that the city may have undertaken, or periodic reports on the expansion of data collection points, the infrastructure being used to collect data, etc. A robust CDP should also ensure compliance with National and State level policies such as National Data Sharing and Accessibility Policy (NDSAP), and the Personal Data Protection Bill (2019).
- **Roles and Responsibilities:** The CDP should also define the roles and responsibilities of the key people including the City Data Officer, Data Champions and Data Coordinators. They should work with city leadership to assess and know the potential of data, establish a data culture across the organizations, help with the implementation of the CDP in their respective departments/organizations, aggregating data demand, and ensuring data quality. This will ultimately help in promoting accountability and transparency.



- **Driving Data Collaboration at State and National Level:** Though the CDP may be written for a specific city, there needs to be a close collaboration and integration with State and National Level bodies. The entities involved at various levels should work together seamlessly and adhere to set protocols as prescribed by the Government of India guidelines. A City Data Cell may be formulated to manage the data platforms, provide technical advice to the departments, handhold for dataset contribution as well as capacity building of Data Coordinators and CDOs.
- **City Data Alliance (CDA):** The CDA will provide a collaborative framework to create and define use cases to solve critical city problems using data and undertake continuous dialogue between various stakeholders in the city around the CDP to inform and evolve it effectively. Key stakeholders should come together to set up a City Data Alliance to assess, strategize, plan, implement and review the CDP, including government agencies, industry, academies, citizens and communities. This will help in keeping the CDP relevant and updated.

25. City Data Policy: A living document

City Data Policy is an instrument that may require changes from time to time. City data policy is not a static document and it can be altered. It is known as a living document or a dynamic document that is continually edited and updated. City Data Policy is called "flexible and rigid" as it is open to changes. Since the data policy has been envisaged keeping in consideration that there will be future changes in technology which might cause certain amendments. The process of presenting/ changing the data policy will be as per standing committee where in the policies will be ratified and amended. This may or may not have a framework for updates, changes or adjustments. This type of document can change away from its original purpose through multiple controlled edits without proper context. This encourages open collaboration with all the stakeholders but in some cases, there can be stagnation if none of the organization takes on the initiative of updating the work/ document. The data organizational structure can be changed if required in the future.

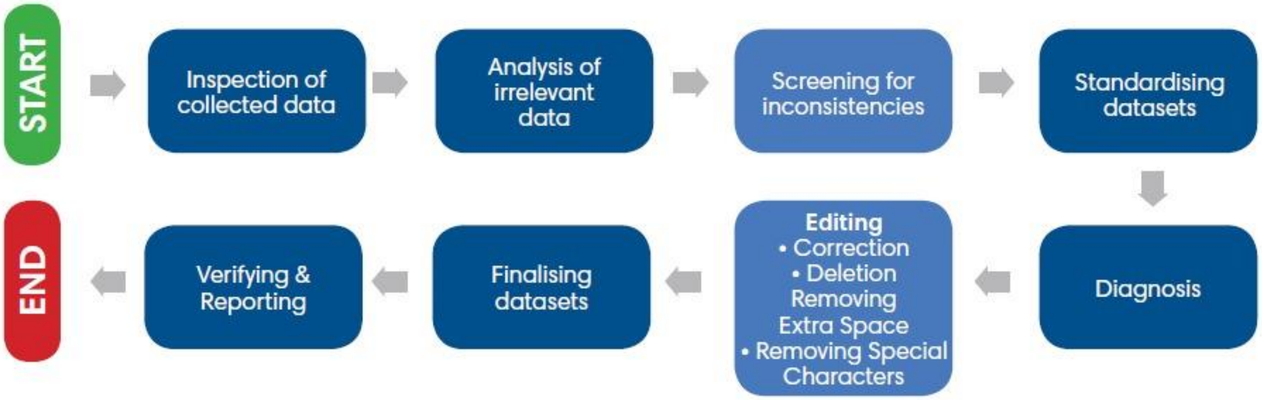
Process of amendment in the city data policy:

- Change request justification
- Justification process
- Approval from standing committee
- Revision

Suggested types of amendments which can be done are as follows:

- Technical amendments
- Differing interpretations
- Addition/ modification/ deletion of clauses in the existing data policy
- Addition/ modification/ deletion of Stakeholders/ data sets/ way of integration

26. SOP for the Data Management



26.1. SOP for Data Collection

26.1.1.SOP for collecting data through API Level Integration

Step 1: Data authority to define the types of data which shall be required from the system
Step 2: Once defined, data to be collected based on API Level integration

Step 3: For 3rd party integrations, data sets to be pre-defined and process shall be approved through a data authority
Step 4: Data authority to evaluate and define the sources of data collection, frequency of data, storage methods, and the checks that should be in place to maintain the accuracy and privacy of such data
Step 5: APIs once finalized shall be shared and sample testing shall be done of the data
Step 6: Upon receival of the data, the same shall be placed into the production environment
Step 7: The APIs shall be documented and finalized

26.1.2.SOP for collecting data through Excel Based Upload Mechanism

Step 1: Excel format of the data to be shared if datasets as identified by city data authority do not have a system
Step 2: Template to be shared by Bhubaneswar Smart City Limited and to be made available in the city dashboard
Step 3: City Data Officer to download and submit the same
Step 4: In case the same is not provisioned, agency to share the data on the identified mail id or to be placed in a shareable Google Sheet
Step 5: Data Authority to incorporate consent before/at the time of collection of any personal data from citizens, with higher standards of consent being applicable to sensitive Data
Step 6: Data authority to ensure clear provisions about data processing including the identity of the entities that are processing the data, the purpose for which it is being processed, the entities that may access this data among other details

26.1.3.SOP for Quality Assessment of Data

Step 1: City Data officer to define the city project goal to ensure accuracy and consistency across multiple systems
Step 2: Depending upon the volume and variety of data, existing policies to be assessed which includes data access, data security and adherence to compliance guidelines
Step 3: Assessed data to be analyzed and gap between project goal and current data to be measured
Step 4: Design and developing improvement plans based on preceding analysis to be done
Step 5: Comprehension of both technical and project process related changes
Step 6: Each update shall include clear and complete metadata (including a conspicuous contact person), group datasets where appropriate, and address concerns noted via a prominent feedback mechanism.
Step 7: Data with serious accuracy and quality concerns shall be adequately documented to avoid spreading misinformation

26.1.4.SOP for Data Publishing

The SOP to enhance and standardize data publishing is listed below:

Step 1: Data shall be published as per the open data norms and in accordance with the NDSAP
Step 2: The selection of datasets and the data publishing options shall be carefully studied before publishing the data on any of the portals
Step 3: When the data is published, appropriate metadata to be tagged
Step 4: Automated flow of data i.e. data by default mechanism to be given prominent focus to publish more high value datasets in the public domain
Step 5: Machine-to-machine technologies such as APIs, Web Services, data from IoT devices, etc.to be prioritized
Step 6: For published datasets, a proper mechanism for user feedback and grievance redressal shall be defined
Step 7: The same shall help data providers to ensure most relevant datasets are published on the Portal
Step 8: City Data Officer needs to determine the frequency with which each data set is published or archived
Step 9: For datasets that are published routinely, governments shall clarify a change in the definition of parameter of the variable
Step 10: City governments shall also clarify whether datasets are only published digitally, the formats in which they are published digitally, and whether hard copies of the datasets can also be found
Step 11: Concerned stakeholders to be updated about the new guidelines and open data norms
Step 12: The CDO to ensure that the datasets are updated in case if any changes/amendments occur in the source of data i.e. the primary data
Step 13: It shall also be ensured that errors and inconsistencies are removed from the primary data and that the dataset included all the metadata along with referential information
Step 14: Datasets shall directly link to the APIs, so that any changes in the base data are simultaneously reflected in the portals

Step 15: Wherever possible, real-time information updates are recommended as they would maximize
the utility the public can obtain from the information
Step 16: This shall also ensure to have a regular maintenance schedule in place and ensuring compliance with the same

26.1.5.SOP for engaging Stakeholders

Step 1: Arrangement of meeting with concerned stakeholder to discuss on requirement of data from both ends
Step 2: Exchange of data sets shall be pursued amongst the stakeholders
Step 3: Upon receival of data from stakeholders, the data access points need to be analyzed based on restricted, classified, personal or non-personal
Step 4: Partnership is made, and a standard MoU shall be signed across

26.1.6.SOP for Data Analysis

The SOP to enhance and standardize data analysis is listed below:

Step 1: City Data Officer to form the hypothesis which is clear and concise
Step 2: The scale of measurement is decided which can be in the form of nominal scale, ordinal scale, Interval or ratio
Step 3: Data is collected through surveys, collecting subscription and registration of data etc. This could be from primary or secondary source
Step 4: Data is manipulated in several ways and correlation is found in excel
Step 5: The earlier set hypothesis is either accepted or rejected based on the level of significance and the further course of action shall be decided
Step 6: This shall be carried forward either by observations, documents or Interviews
Step 7: Valuable insights area drawn by comparison of datasets and relationships shall be observed
Step 8: Graphical representation of the analyzed data sets shall be done by using color, size, scale, shapes and labels to attract attention to key messages

26.1.7.SOP for Data Monetization

Step 1: A committee comprising of representatives from various departments of BMC/BSCL, Traffic Police, Centre for Environment and Development, Bhubaneswar Police, city educational institutions and market experts shall be formed to be City Data Committee
Step 2: In the context of Right to Information act, this committee shall decide the data which can be monetized, fix the price, and review it from time to time
Step 3: The data to be differentially priced for academic research and commercial used
Step 4: BMC shall create data monetizing platform to help data ecosystem to become self-sustainable
Step 5: BMC could also broker third party in order to benefit from this brokerage

26.2.SOP for Data Identification

Step 1: Level of access of the incoming data is analyzed based on restricted, classified, personal or non-personal

Step 2: City Data Officer shall identify and define source of data collection based on API Level Integration or Excel Based Upload Mechanisms

Step 3: Frequency, availability of the data set shall be identified

Step 4: Data which are not readily available but might be aspired in future needs to be identified

Step 5: Source of accessing such aspired data needs to be defined well

27. List of Data readily available as on date

Sl No.	List of Data	Readily Available	Data Partnership	Privately Owned Data	Aspired Data
1	Transport Data pertaining to accidents on Roads				
2	Traffic Data relating to Average waiting time in each Traffic Junction				
3	Number of cab operators			□	
4	Real time traffic speed data				
5	Energy prices and public usage				
6	Data on Air Quality Index				
7	Water Quality Index Data				
8	Number of slum dwellers in the urban periphery				
9	Public dustbins across town				
10	Street Furniture data				
11	Parking demand data				
12	Data on forecasting Bus Ridership				
13	Criminal Data				
14	Taxi trip data				
15	Traffic Count and Speed Data				

28. Way Forward

Data is the crux of smart cities, however for it to be properly utilized it needs to be properly understood, collected and disseminated to all the stakeholders. Data and advance technologies have helped streamline the approach to development of the urban areas. More thoroughly, data and digital technologies can be used to identify the most pressing issues in a city while also offering possible method to solve the problems. Relevant departments and agencies in the state will play an important role in helping cities achieve this integration implemented by Smart Cities Mission to implement Data Smart Cities Strategy for all the 100 Smart Cities through their governance bodies to leverage the potential of data for solving complex urban problems.

A CDP document aims to promote a technology-based culture of data management as well as data sharing and access within organizations/ departments. It is a carefully thought of system of norms to guide decisions and achieve rational outcomes from the data available in the city. It proactively opens up the data, which could be further utilized for developmental purposes and solving urban challenges. Cities should continue the process of evolving the policy further, keeping in tune with the technological advancements and the National, State and City requirements.

The contribution of this work to the urban planning research and practice is multifaced. First, it refers to the analysis of the themes covered by urban plans to the new “data layer” generated by smart city technologies and data-related actions in the city, outlining a research space for further factual and theoretical investigations on this topic in planning research. Second, the prototyping and execution of City Data Plans can be interpreted as future paths for an active shift in urban planning practices to the domain of smart city Programmes. In this sense, the development of the CDP concept is an example of knowledge transfer between two domains i.e. urban planning and smart city in which urban planning knowledge is recognized as generative for new solutions to current problems posed by the deployment of smart city technologies in urban environments.

Annexure A: ISO Norms

ISO 27701: The standard for data privacy

ISO 27701 is the standard in data privacy management. It is the international standard for information security, as it bolts privacy processing controls into the existing framework. It related to the way the organization collects data and prevents unauthorized use or disclosure. It is responsible for creating privacy notices, implementing mechanisms to ensure that individuals can exercise the data subject rights and adopting measures to ensure the data processing meets the GDPR's (General Data Protection Regulation) principle of privacy by design and by default

ISO 27001: 2013 Clause 5.2 – Information security policies and information security policies

Top management must establish an information security policy that is appropriate to the purpose of the organization and must include information security objectives or provides the framework for setting information security objectives. It must also include a commitment to satisfy applicable requirements related to information security and a commitment to continual improvement of the information security management system. The information security policy should be available as documented information. It must be communicated within the organization and be available to interested parties, as appropriate.

Purpose

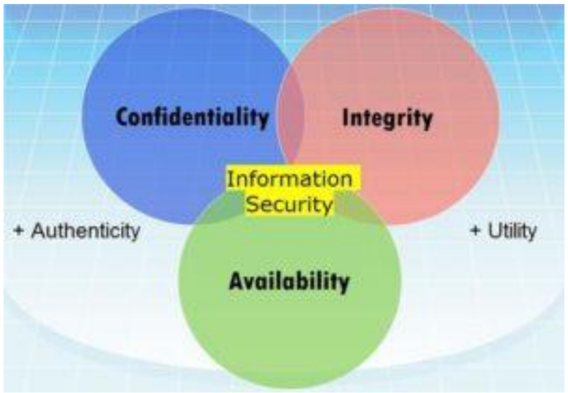
- To establish a general approach to information security
- To detect and forestall the compromise of information security such as misuse of data, networks, computer systems, and applications.
- To protect the reputation of the company with respect to its ethical and legal responsibilities.
- To observe the rights of the customers; providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliance with the policy is one way to achieve this objective

Scope

It should address all data, programs, systems, facilities, other tech infrastructure, users of technology and third parties in a given organization, without exception

Information security objectives

- Confidentiality – data and information assets must be confined to people authorized to access and not be disclosed to others;
- Integrity – keeping the data intact, complete and accurate, and IT systems operational;
- Availability – an objective indicating that information or system is at disposal of authorized users when needed.



Authority and Access Control Policy

Policy refinement takes place simultaneously with defining the administrative control, or authority. In essence, it is the hierarchy-based delegation of control in which one may have authority over his own work, the project manager has authority over project files belonging to a group he is appointed to, and the system administrator has authority solely over system files – a structure reminiscent of the separation of powers doctrine. Access to company's network and servers, whether or not in the physical sense of the word, should be via unique logins that require authentication in the form of either password, biometrics, ID cards, or tokens, etc. Monitoring on all systems must be implemented to record login attempts (both successful ones and failures) and exact date and time of logon and logoff.

Classification of Data

- High-Risk Class – data protected by state and federal legislation (the Data Protection Act, HIPAA, FERPA) as well as financial, payroll, and personnel (privacy requirements) are included here.
- Confidential Class – the data in this class do not enjoy the privilege of being under the wing of law, but the data owner judges that it should be protected against unauthorized disclosure.
- Class Public – This information can be freely distributed. Data owners should determine both the data classification and the exact measures a data custodian needs to take to preserve the integrity in accordance with that level.

Data support and Operations

- The regulation of general system mechanisms responsible for data protection
- The data backup
- Movement of data

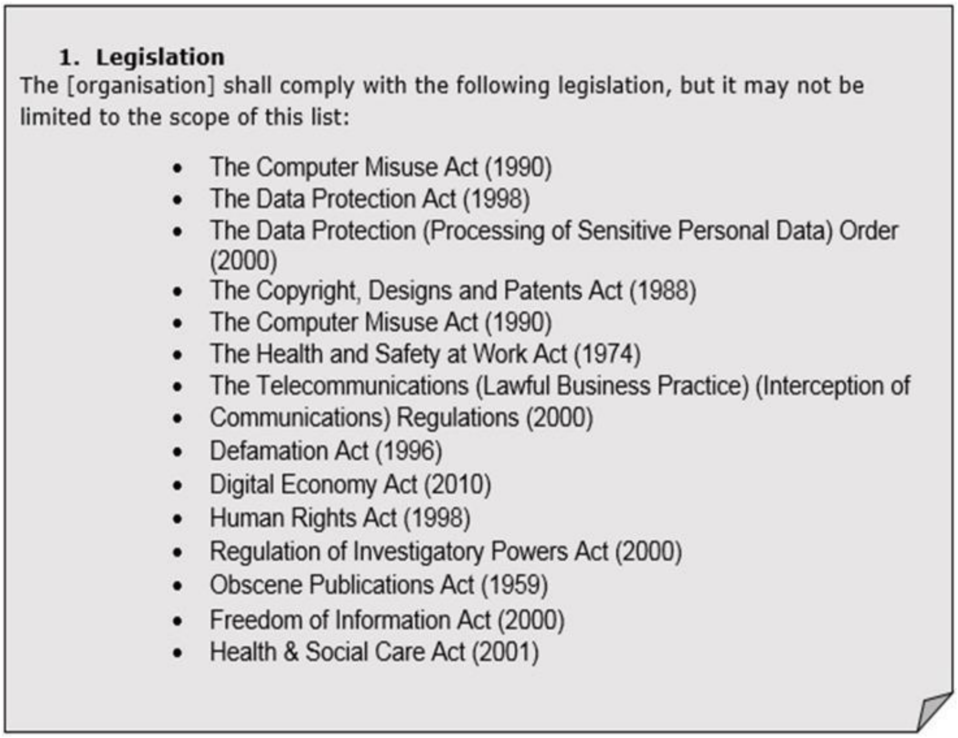
Security Awareness Sessions

Sharing data security policies with staff is one of the most important steps. Making them read/ understand and sign to acknowledge a document does not necessarily mean that they are familiar with and understand the data policies. A training session would engage employees in a positive way to data security, which will ensure that they get a notion of the procedures and mechanisms in place to protect the data, for instance, levels of confidentiality and data sensitivity issues. Such an awareness training should touch on a broad scope of vital topics: how to collect/use/delete data, maintain data quality, records management, confidentiality, privacy, appropriate utilization of overall systems, correct usage social networking, etc. A small test at the end is perhaps a good idea to check their grasp over the norms.

Responsibilities, Rights and Duties of Personnel

General considerations to be taken are responsibility of persons appointed to carry out the implementation, education, incident response, user access reviews, and periodic updates. Prevention of theft, information know-how and project/ departmental confidential information that could benefit competitors are among the most cited reasons.

Reference to Relevant Legislation



1. Legislation

The [organisation] shall comply with the following legislation, but it may not be limited to the scope of this list:

- The Computer Misuse Act (1990)
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- The Telecommunications (Lawful Business Practice) (Interception of
- Communications) Regulations (2000)
- Defamation Act (1996)
- Digital Economy Act (2010)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Obscene Publications Act (1959)
- Freedom of Information Act (2000)
- Health & Social Care Act (2001)

Annexure B: National and State Policies

India – Data Protection Overview

In 2011, the Government of India issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('SPDI Rules'). The SPDI Rules require companies to have a privacy policy, obtain consent when collecting or transferring sensitive personal data or information, and inform the data subject of recipients of such collected data.

The Information Technology Act, 2000 ('IT Act') mandates that bodies corporate, such as companies, firms, sole proprietorships, and other associations of individuals engaged in commercial or professional activities, that handle sensitive personal data or information, are liable to pay damages for any loss caused by their negligence in implementing and maintaining reasonable security practices and procedures. While the IT Act is silent on what constitutes 'reasonable security practices and procedures,' the SPDI Rules offer examples of these standards without providing a clear-cut definition. The IT Act also prescribes criminal penalties, that include both, imprisonment of up to three years and a fine for persons, including intermediaries, who disclose personal information without the consent of the person to whom the data relates, in breach of a relevant contract, or to cause wrongful loss or gain.

The overall protection policies abide by the mentioned broad categories below

Sensitive or Personal Data/ Information

Sensitive or personal information or data' is defined as

- Passwords
- Financial information
- Physical, physiological or mental health conditions
- Sexual orientation
- Medical records and history
- Biometric information

Any detail retaining Moreover, it does not include any personal data that is freely available or accessible in the public domain, or furnished under the Right to Information Act, 2005 or under any other law in force.

Consent and Opting Out

In general, consent forms the most essential element of the scheme of the SPDI Rules. If such consent is obtained by virtue of a standard form contract, then the terms of the contract must be reasonable. Under the SPDI Rules, the provider of data should have an option to opt out of providing the data or information that is being sought by bodies corporate. Providers of information should have this option at all times while availing themselves of services from bodies corporate, as well as have an option to withdraw consent that might have been given earlier. Unlike many other jurisdictions, should providers not consent to the collection of information or otherwise withdraw their consent, the SPDI Rules allow bodies corporate not to provide goods or services for which the information was sought. In addition to the right to opt out of sharing information, information providers have the right to review the information they have provided and to seek the correction or amendment of such information if incorrect.

Privacy and disclosure of information

The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. It should be clear and easily accessible statements of its practices and policies, type of personal or sensitive personal data or information collected under the sensitive or personal data/ information (Section 21.1.1), purpose of collection and usage of such information, disclosure of information including sensitive personal data or information, reasonable security practices and procedures.

Collection of Information

- Body corporate or any person shall obtain consent in writing through letter or Fax or email from the provider of the sensitive data or information regarding purpose of usage before collection of such information.
- Body corporate or any person shall not collect sensitive personal data or information unless —

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

- While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, reasonable to ensure that the person concerned is having the knowledge of —

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and

(d) the name and address of —

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.

- Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force. The information collected shall be used for the purpose for which it has been collected.

- Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be deficient shall be corrected or amended as feasible: Provided that a body corporate shall not be responsible for the authenticity of the sensitive personal data or information supplied by the provider of information to such boy corporate
- Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.
- Body corporate or any person on its behalf shall keep the information secure as provided in rule: Reasonable security practices and procedures
- Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month ' from the date of receipt of grievance.

Transfer of information

A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

Reasonable Security Practices and Procedures

1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security Programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law,

that they have implemented security control measures as per their documented information security Programme and information security policies.

2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).
3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.
4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

Odisha State Data Center Policy- 2020

Vision: Odisha aims to emerge amongst the top five “Datacenter Hubs” in India by 2025 through strategic partnerships, favorable ecosystems, investment, and policy interventions.

The objective of initiating Odisha State Data Center Policy are as follows:

- Develop Odisha into a major “ Datacenter Hub” by 2025
- To attract investors and make Odisha the destination of choice in the sector
- Create enabling and supporting ecosystem that facilitates at least ten medium to large scale data center in the next five years
- To provide IT/ITeS companies with the best business climate
- Create a robust institutional framework for effective implementation, monitoring, and evaluation of this policy

Strategies envisaged by Odisha are:

- Support Research & Development, Innovation, and Entrepreneurship in IT/ ITeS Sector
- ICT Policy encouraging usage of various emerging technologies such as AR, VR, AI, IoT, ML, Animation, Gaming, Robotics, and cloud computing, etc.
- Provide industry-grade skill up-gradation and training to the students to suit the requirements of industry and for obtaining gainful employment.

The Personal Data Protection Bill, 2018 ("Bill") and the Data Protection Committee's ("Committee") Report (released on 27 July 2018) contains the framework and the policymakers' insight on the protection of personal data in India. The recent Draft e-commerce policy indicates the Government's thought process on storing data in India. The Reserve Bank of India (RBI) in April 2020 mandates that all data generated by the payment systems in India has to be stored in India. To fulfill the data localization regulatory requirement, Data Centers needs to be established, regulated, and function under this law by the Odisha Government. Initially, the demand for companies to host their data in India stemmed from a security perspective. The major issues with data localization are not only of cybersecurity but also jurisdiction.

The State Government has placed emerging technologies as a key focus area in the State ICT Policy-2020. The following specialized areas have been identified under emerging technologies in State ICT Policy-2020.

- Cloud Computing
- Artificial Intelligence
- Data Analytics
- Internet of Things (IoT)
- Image Processing
- Blockchain
- Cyber Security
- Virtual/Augmented Reality
- 3D Printing
- Robotics
- Unmanned Aerial Vehicles (UAV)

The State Government offers the following facilities to industries/ entrepreneur for the development of solutions based on the identified areas in State ICT Policy 2020 which are as follows:

Development of a technology-based solution for sector-specific areas such as Health/Education/Social Security’s etc.- Incentives as per the applicable policy of that sector and IPR/Start-up/ICT Policy.

Setting up of R & D and product innovation Centre of Excellence (CoE) on emerging technologies -Incentives as per Industry Policy, Start-Up Policy, and ICT policy.

Special incentives for Product based development in emerging technologies as per identified policies.