Gujarat State Data Governance Framework

Government of Gujarat
Department of Science and Technology
G.R. No: DST/DGV/e-file/24/2026/0376/E-Governance
Sachivalaya, Gandhinagar

Read:

1. **Department of Science & Technology's GR No: DST/DGT/e-file/24/2024/1406/E-Governance, dated 10.12.2024.**
2. **Department of Science & Technology's GR No: DST/DGT/e-file/24/2025/0581/E-Governance, dated 24.07.2025.**
3. **Department of Science & Technology's GR No: DST/DGT/E-file/24/2024/1406/E-Governance dated, 31.12.2025.**

Preamble:

Whereas, under the “Data” pillar of the Gujarat AI Action Plan, provision has been made for the development and publication of a State-level Data Governance Framework to ensure structured governance, protection, sharing, and responsible use of government data; and whereas, in pursuance of the said provision, the Department of Science and Technology, Government of Gujarat has prepared the Gujarat State Data Governance Framework for its adoption and phased implementation.

The Gujarat State Data Governance Framework provides the policy and governance basis for classification, protection, sharing, stewardship, accountability, consent management, monitoring, and audit of datasets handled by government entities.

Resolution:

After careful consideration, the Government is pleased to publish the Gujarat State Data Governance Framework for adoption across all Departments, Boards, Corporations, Authorities, Missions, Societies, and Agencies of the Government of Gujarat.

The Gujarat State Data Governance Framework, enclosed herewith, shall serve as the State-level guiding framework for classification, governance, protection, sharing, interoperability, accountability, consent management, monitoring, and audit of government datasets. The said framework shall operate in consonance with the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules 2025, the Information Technology Act, 2000 (as amended), the National Data Sharing and Accessibility Policy 2012, and other applicable laws and regulations. In case of any conflict between this framework and any applicable law, the provisions of such law shall prevail.

The Government further directs that all concerned entities shall undertake necessary steps for implementation and ensure compliance with the Gujarat State Data Governance Framework.

This issues with the approval of the Government on file no. ICT/IDT/e-file/258/2025/0513/DeepTech Cell dated 06/03/2026.

By order and in the name of the Governor of Gujarat.

(R. C. Desai)

File No: DST/DGV/e-file/24/2026/0376/E-Governance
Approved By: Secretary,DST

Deputy Secretary,
Science & Technology Department
Government of Gujarat

Enclosure:

Gujarat State Data Governance Framework

To,

- PS to Hon. Governor, Rajbhavan, Gandhinagar.
- PS to Hon. Chief Minister, Sachivalaya, Gandhinagar.
- PS to Hon. Minister, Science & Technology Department, Gandhinagar.
- Chief Secretary, Gujarat State, Gandhinagar.
- Secretary, Deparmtent of Science and Technology
- ACS/PS/Secretary to all Departments, Sachivalaya, Gandhinagar.
- JS/DS/US, Science & Technology Department, Sachivalaya, Gandhinagar.
- Director, Directorate of ICT and e-Governance, Gandhinagar.
- All offices under the Science & Technology Department, Sachivalaya, Gandhinagar.
- All branches of the Science & Technology Department, Sachivalaya, Gandhinagar.
- Select File.

File No: DST/DGV/e-file/24/2026/0376/E-Governance
Approved By: Secretary,DST

Gujarat State Data Governance Framework

Department of Science & Technology
Government of Gujarat

Contents

1 Preamble

The Government of Gujarat recognizes data as a strategic asset and a vital enabler for effective governance, inclusive growth, innovation, and sustainable socio-economic development. With rapid growth in digital platforms, smart infrastructure, and connected services, the volume and variety of data generated by various government departments, agencies, and stakeholders are increasing exponentially. The exponential growth of data generated through government departments, public institutions, businesses, and citizens presents both opportunities and responsibilities.

To harness the transformative potential of data, it is imperative to establish a robust governance framework that ensures data is collected, managed, shared, and utilized in a secure, ethical, and transparent manner. This framework represents the Government's vision of building a unified and trusted data ecosystem where non-personal data is treated as a public resource that fuels growth, transparency, and innovation while personal data is managed with the highest standards of trust and privacy.

The Gujarat State Data Governance Framework, mentioned in AI Action Plan*, Sec. 1.1,* as suggested by the *AI Task Force*, is framed with the vision of creating a unified, interoperable, and resilient data ecosystem. This ecosystem will empower government departments, industry, academia, and citizens to responsibly access and leverage data, while upholding the principles of integrity, equity, security, and confidentiality.

Through this framework, the State aspires to position Gujarat as a leader in digital governance by adopting international best practices in data management, encouraging data-driven entrepreneurship and ensuring that the benefits of data are equitably shared across all sections of society. This framework reflects the Government's commitment to safeguarding the rights of citizens, promoting digital trust, and advancing Gujarat's journey towards becoming a knowledge-driven, innovation-led, and future-ready economy.

2 Guiding Principles

The Gujarat State Data Governance Framework shall be guided by the following ten principles to ensure effective, ethical, and responsible use of data:

A. Accountability and Transparency

Establish clear roles and responsibilities for all stakeholders in data collection, management, and usage. Enable transparency in data-driven decision-making while upholding confidentiality, integrity and privacy requirements.

B. Citizen-Centricity

Place citizens at the core of all data governance initiatives. Ensure that data usage enhances service delivery, protects rights, and improves the overall quality of life of citizens.

C. Data Integrity and Quality

Ensure that data is accurate, complete, timely, consistent, and reliable. Adopt standardized formats, taxonomies and metadata frameworks to maintain uniformity across departments.

D. Privacy and Security

Safeguard personal data in compliance with applicable laws and regulations. Implement robust cybersecurity, encryption, and access-control mechanisms to prevent misuse, unauthorized access, and breaches.

E. Interoperability and Standardization

Promote the use of open standards, protocols, and platforms to ensure seamless integration and exchange of data across government departments and external stakeholders. Facilitate cross-sectoral collaboration through common data exchange frameworks.

F. Ethical Use of Data

Ensure that data is used responsibly, fairly, and without discrimination. Prevent misuse of data for profiling, surveillance, or purposes contrary to public interest.

G. Open Data and Innovation

Encourage sharing of non-personal, anonymized data for public use, research and innovation. Foster entrepreneurship, start-ups, and academia through open data initiatives while ensuring citizen trust.

H. Resilience and Sustainability

Build a resilient data infrastructure capable of withstanding technological disruptions, cyber threats, and future demands. Promote sustainable practices in data storage, management, and utilization.

I. Compliance with Legal and Regulatory Frameworks

Align with national data protection, cybersecurity, and IT governance laws and standards. Ensure Gujarat's data governance ecosystem is adaptive to evolving legal, technological, and societal requirements.

J. Capacity Building and Awareness

Develop institutional capacity, skillsets, and digital literacy across government entities to ensure effective implementation of this data governance framework. Conduct awareness programs to promote responsible data use among citizens and stakeholders.

3 Definitions

#	Particular	Definition
1	Data	Refers to any representation of facts, numbers, characters, images, sound, or any combination thereof, which can be processed, stored, or transmitted electronically.
2	Personal Data	Any data that relates to an identified or identifiable natural person, including but not limited to name, address, contact details, identification number, or location data and shall have the meaning assigned under the Digital Personal Data Protection Act, 2023.
3	Sensitive Personal Data	A category of personal data that includes information such as financial details, health records, biometric identifiers, caste, religion, or any other data classified as sensitive under applicable laws/Rules/Guidelines.
4	Anonymized Data	Data that has been processed to irreversibly prevent identification of the data principal, such that it cannot be linked to an individual by any means reasonably likely to be used.
5	Open Data	Data that is made available by the Government of Gujarat, in machine-readable formats, free of charge or under specified terms of use, for access, reuse, and redistribution by the public.
6	Data Principal	The individual to whom the personal data relates.
7	Data Fiduciary	Any government department, agency, or entity that determines the purpose and means of processing personal or non-personal data.
7.1	Significant Data Fiduciary	As defined under Section 10 of the DPDP Act, 2023. Includes State Departments designated by the Central Government to adhere to higher obligations like appointing a DPO and conducting periodic Audits.
8	Data Processor	Any entity that processes data on behalf of a Data Fiduciary, including private vendors, contractors, or technology partners engaged by the State.

9	Data Steward / Data Officer	An officer designated within a department/agency responsible for ensuring data quality, integrity, compliance, and adherence to the State's Data Governance Framework.
10	Data Sharing	The act of providing access to data sets across government entities, public institutions, or authorized third parties, in a secure and controlled manner.
11	Data Governance	The overall management framework that defines decision rights, accountability, standards, and processes for the effective and ethical use of data.
12	Interoperability	The ability of different information systems, applications, and processes to communicate, exchange, and use data in a seamless and standardized manner.
13	Metadata	Information that describes the characteristics of data, including structure, format, source, ownership, and context, to facilitate effective management and use. Metadata is the data providing information about one or more aspects of the data.
14	Data Lifecycle	The sequence of stages through which data passes, from collection and storage to usage, sharing, archival, and disposal.
15	Data Ecosystem	The interconnected environment of Data Principals, Data Fiduciary, Data Processors, platforms, standards, and technologies that enable effective governance and utilization of data.
16	Data Breach	An incident where there is an unauthorized access to, disclosure of, alteration of, or destruction of data, potentially compromising confidentiality, integrity, or availability.
17	Data Set	Collection of logically related features, attributes or variables including processed data or information.
18	Digital Public Infrastructure (DPI)	The foundational digital systems, platforms, and registries that enable secure exchange, verification, and usage of data to support governance and innovation.

4 Current Gaps in the E-Governance Ecosystem

Following are the gaps present in the system:

a) **Siloed Data Systems:** Departmental databases function independently with minimal cross-platform integration.
b) **Legacy I.T. Infrastructure:** Outdated systems restrict the adoption of uniform standards and modern technologies. Current applications lack the technical capability to capture, manage, and revoke consent from stakeholders.
c) **Inconsistent Data Quality:** Gaps in accuracy, completeness, and standardization affect reliability.
d) **Privacy and Security Risks:** Expanding digital footprints increase exposure to breaches and non-compliance resulting in potential statutory penalties under the new data protection regime.

5 Future Needs of the Governance Ecosystem

As governance models evolve, the following priorities emerge for the next generation of digital public infrastructure:

a) **Integrated Data Exchange:** Seamless and secure data flow across institutions to support unified citizen services.
b) **Data Sovereignty and Compliance:** Assurance that sensitive information remains within national jurisdiction while meeting legal and regulatory standards.
c) **Citizen Empowerment:** Mechanisms enabling individuals to control access, sharing, and use of their personal data.
d) **Collaboration for Innovation:** Provision of non-personal datasets to academia, start-ups, and industry to support research and economic growth.

A State Data Governance Framework provides the formal framework required to address existing gaps, align with emerging legal mandates, and prepare for future needs of governance. It establishes clarity on ownership, interoperability, accountability, and ethical use of data, ensuring that the digital transformation of governance is inclusive, transparent, and sustainable.

6 Need for Data Governance Framework

Over the past few decades, state's e-governance ecosystem has undergone significant and transformation under the Digital India initiative. The rapid establishment and expansion of digital systems have also resulted in the generation of vast, diverse and complex datasets. In the absence of structured frameworks, these datasets often remain fragmented across departments, leading to duplication, inconsistencies, and barriers to effective use. Legacy infrastructure, variations in data quality, and lack of interoperability further limit the potential of data-driven

decision-making. At the same time, rising concerns over data privacy, security, and accountability have reinforced the need for a comprehensive data governance approach aligned with the national and global best practices.

7 Vision

To establish Gujarat as a trusted, secure, and innovation-driven data ecosystem where Non-Personal Data is treated as a strategic public asset and Personal Data is secured as a position of trust. The vision is to enable transparent, citizen-centric governance through secure, ethical, and interoperable data practices that strengthen public trust, accelerate socio-economic development, and promote evidence-based decision-making.

8 Mission

To build a unified and resilient State data environment that:

a) Ensures privacy and protection of personal data in compliance with national laws;
b) Promotes standardized, high-quality, and interoperable data across departments;
c) Enables responsible data sharing and reuse for improving governance and service delivery;
d) Facilitates innovation and economic growth by providing secure access to non-sensitive data;
e) Strengthens institutional capacities for data stewardship, analytics, and governance;
f) Encourages ethical and transparent use of data to foster digital trust..

9 Objectives

The State Data Governance Framework aims to:

A. Establish a Strong Governance Structure

Create clear policies, standards, and institutional mechanisms that define ownership, accountability, and decision rights for all data stakeholders.

B. Ensure Data Privacy, Quality, and Security

Implement robust controls for protecting personal and sensitive data while ensuring accuracy, completeness, and integrity of all government datasets.

C. Enable Interoperability and Responsible Data Sharing

Promote standardized data models, metadata, and APIs to ensure seamless, secure exchange of data across departments and authorized stakeholders.

D. Accelerate Data-Driven Governance

Support evidence-based decision-making using analytics, AI/ML, and emerging technologies to improve service delivery and policy formulation.

E. Promote Open Data and Innovation

Provide anonymized and non-personal datasets for research, entrepreneurship, and public benefit while safeguarding citizen rights.

F. Build Capacity and Strengthen Institutions

Develop skills, awareness, and technical capabilities across government entities to implement the Framework effectively.

G. Ensure Accountability and Transparency

Implement mechanisms for monitoring, auditing, and reporting to enhance public confidence in the State's data ecosystem.

10 Roadmap (5-Year Horizon)

The Framework will be implemented in a phased manner to create a mature, citizen-centric data ecosystem.

A. Phase 1- Foundation & Governance Setup (Year 0 – 1.5)

I. Establish State Data Governance Committee and Departmental Committees

II. Conduct modernization and standardization of legacy data systems

III. Implement data classification, metadata standards, and State Data Catalogue

IV. Establish consent management system aligned with DPDP Act

V. Roll out interoperability standards, APIs, and data-sharing mechanisms

VI. Institutionalization of audits, compliance programs, and continuous improvement

VII. Ensure compliance with DPDP Act

VIII. Expand coverage across all departments and agencies

B. Phase 2- Integration & Interoperability (Year 1.5 – 3)

I. Implement initial open data portals and secure shared data repositories

II. Introduce Golden Record initiatives and master data management (MDM)

C. Phase 3- Expansion & Innovation (Year 3–5)

I. Launch analytics platforms and predictive governance initiatives

II. Promote collaboration with industry and academia using non-sensitive datasets

III. Introduce use of emerging technologies (AI, Blockchain, IoT, Edge) for secure data exchange

D. Phase 4- Consolidation & Maturity (End of Year 5)

I. Fully integrated State data ecosystem with mature governance processes

II. Strengthened cyber-security and resilience frameworks

11 Scope and Applicability

The Gujarat State Data Governance Framework shall provide a comprehensive framework for the collection, storage, management, sharing, protection, and ethical use of data generated, maintained, or processed by government entities and their stakeholders. Its provisions shall extend to the following domains:

A. Applicability to Government Entities

This framework should apply to the following Govt. bodies/institution:

i. All Departments, Boards, Corporations, Authorities, Missions, Societies, and Agencies of the Government of Gujarat.
ii. All Urban Local Bodies (ULBs), Panchayati Raj Institutions (PRIs), and other Local Self-Government Institutions functioning under the State Government.
iii. All State Public Sector Undertakings (State-PSUs), State-run Institutions, and Autonomous Bodies established by or under the control of the Government of Gujarat.

B. Applicability to Data Lifecycle

This framework shall apply to all stages of the data lifecycle, including but not limited to:

i. Data collection and generation,
ii. Data storage and classification,
iii. Data processing and analysis,
iv. Data sharing, reuse, and publication,
v. Data security and privacy, and
vi. Data archival, retention, and disposal.

C. Applicability to Stakeholders

This framework shall apply to all the stakeholders below:

i. **Government Departments and Agencies:** As primary Data Fiduciaries responsible for compliance.
ii. **Private Sector and Technology Partners**: Engaged as Data Processors under contract with State entities, bound by this framework and relevant laws.

iii. **Academic and Research Institutions**: Authorized to access non-personal or anonymized datasets for innovation and public good.
iv. **Citizens**: As Data Principals, whose rights and privacy shall be protected under this framework and the DPDP Act, 2023.
v. **Others**: Any other entity processing data provided by Government of Gujarat.

D. Geographical Applicability

The domain and boundaries of applicability:

i. This data governance framework shall extend to all territories under the jurisdiction of the Government of Gujarat.
ii. It shall apply to data hosted within the State, as well as data processed on behalf of the State by third parties located in India or outside India, subject to compliance with national legal requirements.

E. Legal and Regulatory Alignment

This data governance framework shall operate in consonance with the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000 (as amended), National Data Sharing and Accessibility Policy, 2012, and other applicable laws and regulations. In case of any conflict between this framework and a central law, the provisions of the central law shall prevail.

12 Core Components of Data Governance

A. Data Classification

To ensure effective management, protection, and utilization of data, all data under the purview of the Government of Gujarat shall be classified according to its sensitivity, privacy requirements, and intended use. The classification framework provides a structured approach to assign responsibilities, security controls, and sharing guidelines.

1. Open Data

a) **Definition**: Data that is non-sensitive in nature and may be freely shared with the public without restriction.
b) **Examples**: Statistical reports, aggregated indicators, anonymized datasets, general geographic information, service performance dashboards.
c) **Access**: Freely accessible through open data portals or publications.

2. Sharable Data

a) **Definition**: Data that is not covered under the negative list and is non-sensitive, but may require formal request, registration, or authorization before use.
b) **Examples**: Departmental datasets for academic research, anonymized administrative records, sector-specific registries.
c) **Access**: Available to government entities, research institutions, and industry partners under defined processes.

3. Restricted Data

a) **Definition**: Data whose access is limited to authorized users due to its sensitivity, operational importance, or security implications.
b) **Examples**: Departmental beneficiary databases, real-time service logs, internal government communications.
c) **Access**: Allowed only through a prescribed registration, approval, or clearance process.

4. Sensitive Data

a) **Definition**: Data that relates to personal information or critical government functions and is governed by the Digital Personal Data Protection Act, 2023 and other applicable legal frameworks.
b) **Examples**: Personal identification details (e.g., Aadhaar-linked records), health records, financial information, law enforcement and security data.
c) **Access**: Strictly regulated; subject to consent, anonymization, encryption, and compliance with statutory provisions.

5. Negative List Data

a) **Definition**: Data explicitly designated as non-sharable by the concerned department or organization, typically on grounds of privacy, security, or sovereignty.
b) **Examples**: Classified records, confidential government files, data pertaining to national security.
c) **Access**: Not available for sharing under any circumstances, unless directed by law.

6. Transactional Data

a) **Definition:** Data generated in real time during service delivery or administrative transactions, requiring secure storage, monitoring, and periodic review.
b) **Examples:** Financial transactions, citizen service requests, e-office logs, digital identity authentications.
c) **Access:** Subject to departmental authorization, retention policies, and audit mechanisms.

B. Data Classification Process

Following are to be followed to classify the data:

i. Each department shall classify its datasets at the point of creation or acquisition, in accordance with this framework.
ii. Data Owners shall be responsible for periodic review and reclassification of datasets based on changes in sensitivity, legal requirements, or usage patterns.
iii. All classifications shall be documented in the State Data Catalogue, along with applicable access protocols.

iv. Appeals or disputes regarding classification shall be addressed by the designated State Data Governance Authority.
v. Ensure the completeness, accuracy and consistency of personal data.

C. Data Protection

All contracts involving state datasets shall include provisions requiring detailing of retention, returning or deleting datasets and derived artefacts upon contract termination, prohibiting derivative commercialization without SDA approval, and recognizing State stewardship and compliance monitoring.

Under the Data Governance Framework, the State Data Authority (SDA) shall prescribe a mandatory Standard Data Processing Addendum (DPA) template. This DPA shall be mandatorily incorporated into all Government tenders, contracts, and engagements involving the processing of personal data. The Standard DPA shall, at a minimum, provide for:

(i) A breach notification obligation requiring the vendor to report any personal data breach to the State within six (6) hours of becoming aware of such breach;
(ii) Full indemnification of the State against any penalties, liabilities, or damages arising from vendor negligence, non-compliance, or breach of applicable data protection obligations;
(iii) An explicit right of the State to audit, or cause to be audited, the vendor's systems, processes, and controls relevant to data processing and data security.

D. Ownership of Data

I. Citizen Ownership of Personal Data

a. As per the Digital Personal Data Protection Act, 2023, the Data Principal (citizen) is the ultimate owner of their personal data.
b. The Government of Gujarat, its departments, agencies, and affiliated institutions shall act only as Data Fiduciaries or Data Processors, holding and processing personal data in trust, strictly for lawful and defined purposes.
c. Citizens retain full rights over their personal data, including the rights of access, correction, erasure, and grievance redressal, as provided under the national law.

II. Government Custodianship of Non-Personal Data

a. All non-personal and anonymized data generated, collected, or compiled by State departments, agencies, or institutions shall be treated as a strategic public resource.
b. The Government of Gujarat shall exercise custodianship over such data, ensuring its availability for policymaking, governance improvement, innovation, and research.
c. Departments and agencies generating such data shall be responsible for its stewardship, quality, and controlled sharing under this framework.

III. Open Data Ownership

a. Non-sensitive, non-personal data designated as Open Data shall remain under the ownership of the Government of Gujarat but will be made accessible for public use under an appropriate open framework.
b. Such ownership shall not restrict reuse by citizens, entrepreneurs, start-ups, or academia, provided it is within the scope of the terms of use defined by the State.

IV. Shared and Federated Data Ownership

a) For datasets created collaboratively between the State Government and external stakeholders (e.g., industry partners, academic institutions, or other States), ownership shall be determined based on mutually agreed data-sharing agreements.
b) The State shall retain custodial rights to ensure that such data is not misused and continues to serve the public interest.

13 State Data Governance Institutional Framework

The framework provides a structured governance mechanism to ensure secure, ethical, and effective management of data across the State of Gujarat. It defines roles, responsibilities, processes, and oversight mechanisms to manage data as a strategic asset, while protecting citizen rights.

A. State Data Governance Committee (SDGC) – Apex Body

The SDGC is the highest decision-making body ensuring alignment between data governance framework objectives and operational execution. It balances innovation, transparency, and privacy at the state level.

I. Administrative Framework

a) **Chairperson:** Chief Secretary, Government of Gujarat
b) **Convenor-cum-Member:** ACS/PS/Secretary, Department of Science & Technology (DST) – Member Secretary
c) **Members:**
    1. ACS/Principal Secretary/Secretary of relevant Departments
    2. Chief Information Security Officer (CISO)
    3. Nodal Data Officers (as required)
    4. Domain experts may be invited as special members

II. Responsibilities:

a) Provide strategic oversight and policy direction for the State Data Governance Framework.
b) Review and approve amendments, updates, and revisions to the Framework.
c) Oversee the overall functioning of the State Data Governance ecosystem.
d) Guide inter-departmental collaboration.

e) Review periodic reports.
f) Facilitate the appointment of the State Chief Data Officer.
g) Ensuring the State's data governance initiatives remain in strict alignment with mandates from Central Government bodies, including the Data Protection Board of India.

B. State Data Authority

A dedicated office responsible for governing, managing, and driving the work envisioned in State Data Governance Framework.

I. Administrative Framework

a) **Chairperson:** ACS/PS/Secretary, Department of Science & Technology
b) **Convenor-cum-Member:** State Chief Data Officer
c) **Members:** Director IT & e-Governance, Chief Information Security Officer (CISO), Nodal Data Officers from each department and domain experts as required

II. Roles and Responsibilities

a) Drive implementation of State Data Governance Framework to accomplish the objectives and ensure adherence to this data governance framework by all departments.
b) Develop and maintain the State Data Catalogue, Data Repository, and Metadata standards.
c) Monitor compliance with the State Data Governance Framework across all departments.
d) State Chief Data Officer will be responsible for timely reporting the data breach to the Data Protection Board of India and ensure compliance with all Government issued Acts, Rules and Regulations.
e) Develop Standard Operating Procedures (SOPs), if required, for the effective implementation of standards notified by the Data Protection Board of India.
f) Facilitate periodic audits and data quality reviews.
g) Facilitate capacity building and training for departmental officers.
h) Promote use of non-sensitive datasets for innovation, research, and public benefit.
i) Serve as the nodal agency for collaboration with industry, academia, and central government on data related matters.

C. Department-Level Data Committee

A decentralized committee within each department to manage data-related responsibilities at the source.

I. Administrative Framework

a) **Chairperson:** ACS/PS/Secretary of the respective Department
b) **Members:**
    i. Departmental Data Officer (DDO)
    ii. Sub-Data Officers (from key directorates/divisions)
    iii. Data Steward (responsible for data handling, storage and security)

iv. Technical Advisor / IT Officer may be appointed/invited as special members

II. Roles and Responsibilities

a) Drive all department level activities to align and accomplish the vision defined in the State Data Governance Framework.
b) Classify departmental datasets into Open, Sharable, Restricted, Sensitive, or Negative List.
c) Maintain and regularly update department-level entries in the State Data Catalogue.
d) Ensure secure collection, storage, and sharing of departmental data.
e) Implement departmental data quality improvement initiatives.
f) Act as the primary point of contact with the State Data Authority.
g) Support innovation and research requests by facilitating data access.
h) Data Committee will be responsible for timely reporting the data breach to the State Chief Data Officer and ensure compliance with all Government issued Acts, Rules and Regulations.
i) A comprehensive Data Retention and Archival Policy should be formulated and reviewed periodically at department level to ensure continued relevance and compliance with legal, administrative, and operational requirements.

D. Supporting Mechanisms

In addition to the above administrative structure below roles will be necessary for appropriate implementation of this framework:

I. **Technical Support Unit:** A specialized unit comprising of domain experts under the State Data Authority to provide technical assistance, audit tools, and advisory services.
II. **Data Steward/Officer – Department-Level Execution:** The Department Head should appoint a **Data Steward/Officer** who are embedded within departments to operationalize data governance at the functional level, ensuring accountability and compliance with the following responsibilities:
    a) Ensure accuracy, integrity, and timeliness of data.
    b) Manage access control, processing permissions, and audit trails.
    c) Serve as primary contact for citizen grievances and consent management.
    d) Classify and manage departmental datasets according to the Data Classification Framework.
    e) Ensure data quality, security, and compliance.
    f) Report all events of data breach to State Chief Data Officer.
    g) Facilitate authorized data sharing.
    h) Maintain departmental metadata and audit logs.
    i) Report periodically to the State Data Authority.

14 Consent Management Framework

A. Citizen Consent

Respecting Data Principal Autonomy and ensuring the ethical use of personal information are central to this framework. Consent serves as the foundation for lawful collection, processing, and sharing of personal data within the State Data Ecosystem.

Consent Management Framework will ensure that Data Principle maintain meaningful control over their personal data while enabling government departments to operate transparently and lawfully. It balances individual rights with legitimate governance needs, fostering trust, accountability, and inclusivity in the State's data ecosystem.

i. Consent Management

a) **Citizen Consent:** Consent Management Portal to be implemented for citizen to grant, update, revoke consent to their data or delete all their data.

ii. Consent Mechanisms

a) **Digital Consent:** Consent shall be captured through digital platforms with clear prompts, consent dashboards, and acknowledgment receipts.
b) **Consent Manager:** Consent processes may be facilitated through registered Consent Managers (as defined in the DPDP Act, 2023) to ensure transparency and user control.
c) **Multilingual Access:** Consent requests must be provided in local languages to ensure inclusivity and comprehension.
d) As defined in DPDP Act 2023 and Digital Personal Data Protection Rules, 2025 (Subject to the compliance to DPDP Act),The State and any of its instrumentalities may process personal data of a Data Principal for any of following uses, namely - to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where–
    a. Data Principal has previously consented to the processing of her personal data by the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or
    b. Such personal data is available in digital form in, or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government.

    Where processing is to be done under above mentioned condition, the same is undertaken while giving the Data Principal an intimation in respect of the same and—
    c. giving the business contact information of a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data;
    d. specifying the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if

any, using which such Data Principal may exercise her rights under the DPDP Act; and

e. is carried on in a manner consistent with such other standards as may be applicable to the processing of such personal data under policy issued by the Central Government or any law for the time being in force;

iii. Citizen Rights

a) **Right to Information:** Citizens must be informed of who is collecting the data, why it is being collected, how it will be used, and with whom it will be shared.
b) **Right to Review:** Citizens shall have access to a consent dashboard to view active consents, past approvals, and data usage history.
c) **Right to Withdraw:** Withdrawal of consent shall not affect access to essential services; however, certain optional services may be discontinued where data is required.
d) **Right to Correction and Erasure:** Citizens may request rectification or deletion of their personal data where applicable.

(e) Departmental Responsibilities. Each Departmental Data Committee shall:

i. Obtain consent in consent management systems.
ii. Ensure records of consent are securely stored, auditable and traceable.
iii. Report consent violations to the State Data Authority.

B. Exceptions to Consent

In line with the DPDP Act, 2023 and applicable laws, data may be processed without consent in the following limited cases:

i. For compliance with legal obligations of the State.
ii. For responding to medical emergencies or disaster management.
iii. For carrying out functions of the State in the interest of sovereignty, integrity, and security.
iv. For anonymized or aggregated datasets used for statistical, research, or public interest purposes.

C. Consent Manager Architecture

The Consent Manager serves as the critical mechanism for enabling citizens to exercise control over their personal data. It ensures that consent for data collection, use, sharing, and withdrawal is managed in a standardized, transparent, and auditable manner across all departments.

The Framework shall mandate the establishment of a Consent Manager (CM)–compliant gateway by the State. The role of the State shall be limited to that of a Data Fiduciary, responsible for securely interoperating with any Consent Manager registered with the Data Protection Board of India.

i. Design Principles

a) **Interoperability:** Built using open APIs to integrate with departmental systems.
b) **Transparency:** Citizens can view, grant, deny, or withdraw consent at any time.
c) **Accountability:** Consent records are immutable, auditable, and traceable.
d) **Compliance:** Aligned with the Digital Personal Data Protection Act, 2023 and open to integration with national consent frameworks.

ii. Administrative Framework

a) **State Data Authority (SDA):**
   i. The State Data Authority (SDA) shall facilitate adaptation and implementation of the application programming interface (API) standards and technical specifications as notified by the Data Protection Board of India, without modification.
   ii. The State shall encourage an open and competitive consent ecosystem, enabling citizens to interact with government services through any Consent Manager registered with the Data Protection Board of India.

b) **Departments:**
   i. All State departments shall expose and maintain standardized APIs to enable interoperability and secure connectivity with any duly licensed Consent Manager (CM).
   ii. Ensure departmental datasets respect the consent status before any data processing or sharing.

c) **Citizens (Data Principles):**
   i. Access the Consent management portal to view active consents, grant, modify or revoke consent. Track data use history and delete their data.

d) Governance
   i. The State Data Authority will facilitate periodic audits of the Consent Management.
   ii. Departments are required to publish transparency reports detailing consent-based data use.
   iii. Violations of consent rules will be escalated to the State Data Governance Committee for corrective action.

15 Data Protection & Security

Ensuring the confidentiality, integrity, and availability of government data is a fundamental pillar of the State Data Governance Framework. All data generated, collected, or managed under this framework shall be protected through a comprehensive security framework that incorporates legal compliance, international standards, and emerging best practices.

A. Guiding Principles

i. **Privacy by Design:** Protection of personal data must be embedded into every stage of data collection, processing, storage, and sharing.

ii. **Legal Compliance:** All security measures shall conform to the Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, and other applicable national laws.
iii. **Proportionality:** Security controls must be commensurate with the sensitivity and classification of the dataset (Open, Sharable, Restricted, Sensitive, Negative List, Transactional).
iv. **Zero Trust Approach:** Data access shall follow the principle of "never trust, always verify," with continuous authentication and monitoring.
v. **Resilience:** Systems must be designed to withstand and recover rapidly from cyberattacks, natural disasters, or technical failures.

B. Data Protection Measures

For ensuring security of Data, as per requirement of data residency, data transit, encryption and latest available technology, appropriate security measures must be implemented by the Data Fiduciaries. Some measures are illustrated below:

i. **Encryption Standards:**
   a) Data at rest: Minimum AES-256 encryption.
   b) Data in transit: TLS 1.3 or higher.
   c) End-to-end encryption for personal or sensitive and transactional datasets.
   d) All information security and data protection controls shall be designed, implemented, and maintained in accordance with prevailing industry best practices and standards, as notified or prescribed by CERT-In, the Data Protection Board of India, and other relevant Central Government authorities from time to time.

ii. **Access Control:**
   a) Role-based and need-to-know access models.
   b) Multi-Factor Authentication (MFA) for all privileged accounts.
   c) Regular review and revocation of dormant accounts.

iii. **Anonymization and Pseudonymization:**
   a) Personal or sensitive datasets used for analytics, innovation, or public release must undergo anonymization.
   b) Use of pseudonymization where re-identification is required under controlled environments.

iv. **Backup and Recovery:**
   a) Automated, encrypted backups with geographically separated DR sites.
   b) Periodic testing of recovery protocols to ensure readiness.

v. **Incident Management:**
   a) Reporting and coordination with to State Cybersecurity Response Team.
   b) Mandatory breach notification to CERT-In, Data Protection Board of India and affected stakeholders within prescribed timelines.

C. Security Governance

i. **State Data Authority (SDA):**
   a) Prescribes baseline security standards for all departments.
   b) Ensure appointment of Data Protections Officers in compliance with DPDP Act 2023.

c) Facilitate annual audits and publishes compliance status.

ii. **Data Fiduciary:**
   a) Implement data security policies at the departmental level.
   b) Ensure compliance with classification-based controls.
   c) Perform third-party assessments of security infrastructure as and when required.
   d) Perform periodic Audits and Data Protection Impact Assessment as required.
   e) Submit reports to the SDA and the State Data Governance Committee.

D. Citizen-Centric Protection

i. Citizens' personal data shall be processed only with consent, as per DPDP Act, 2023.
ii. Citizens shall have the right to request correction, erasure, or restricted use of their personal data where applicable.
iii. The Consent Management Framework shall be implemented to ensure transparency and accountability.

E. Emerging Technology Safeguards

i. **AI and Analytics:** Any use of AI-based data processing must incorporate fairness, transparency, and auditability.
ii. **Blockchain:** May be used for audit trails in critical data flows to prevent tampering.
iii. **IoT and Edge Devices:** Must comply with device-level encryption, secure firmware updates, and edge security standards.

F. Storage, Retention, and Erasure of Personal Data

To ensure uniform, lawful, and auditable handling of personal data across State departments, the Data Governance Framework shall explicitly address storage, retention, and erasure obligations, including scenarios where statutory retention requirements coexist with a citizen's Right to Erasure.

Accordingly, this Framework shall mandate each Data Fiduciary to develop, implement, and maintain a Data Retention Schedule applicable to the personal data processed under its control. Such Data Retention Schedule shall define the maximum permissible retention periods for different categories of personal data, classified on the basis of purpose of processing, data sensitivity, and applicable legal, regulatory, or statutory requirements. The State Data Authority (SDA) shall provide oversight over such Data Retention Schedules, and may issue standard operating procedures, guidance, or templates, as necessary, to ensure consistency and compliance across departments.

The Retention Schedule shall, at a minimum:

i. Clearly distinguish between primary personal data (core records directly identifying a data principal) and ancillary data (including system logs, access logs, metadata, audit trails, and traffic data).

ii. Prescribe procedures for operationalizing the Right to Erasure, wherein primary personal data is required to be erased upon request while certain associated records may be lawfully retained for a specified duration in accordance with applicable rules.
iii. Ensure that any retained ancillary data following erasure is strictly limited to the minimum necessary for compliance, security, audit, or legal purposes, and is subject to appropriate access controls and safeguards.
iv. Prohibit indefinite or open-ended retention of personal data, unless expressly mandated by law.

16 Implementation Guidelines

The effective execution of the State Data Governance Framework requires a structured, phased, and coordinated approach across all levels of governance. For well-orchestrated implementation, it is useful to define guidelines that bring clarity on the roles, responsibilities, processes, and mechanisms that will govern implementation of this data governance framework.

A. Phased Implementation

The implementation of this Data Governance Framework shall be undertaken in a phased manner, in alignment with the five-year roadmap outlined in detail in Section 10 of this document.

B. Standard Operating Procedures (SOPs)

i. Each department shall adopt SOPs for data classification, storage, security, consent, implementation and sharing, issued by the SDA.
ii. Where this Framework requires departments to adopt Standard Operating Procedures (SOPs), the State Data Authority (SDA) shall, as part of its compliance facilitation role, issue or publish such SOPs, guidance, or templates, where necessary, to support timely and consistent implementation across departments.
iii. SOPs shall be updated periodically to reflect legal, technological, and governance developments.
iv. Compliance with SOPs shall be mandatory and subject to audit.

C. Capacity Building

i. Regular training and certification programs for departmental staff on data governance, privacy, and analytics.
ii. Development of a Knowledge Repository with toolkits, templates, and guidelines.
iii. Collaborate with universities and research institutions to facilitate in education and innovation.

D. Monitoring and Reporting

i. Departments must submit quarterly implementation progress reports to the SDA.

ii. SDA will publish an Annual State Data Report covering progress, compliance status, and recommendations.
iii. Implementation progress shall be linked to Key Performance Indicators (KPIs) defined by the State Data Authority.

E. Funding and Resource Allocation

i. Dedicated budget allocations under the State IT / e-Governance plan shall support implementation.

F. Change Management and Awareness

i. Awareness campaigns will inform citizens about their rights under the data governance framework (consent, privacy, open data access).
ii. Departments shall establish helpdesks to support users and address grievances.
iii. A Change Management Program will ensure departments transition smoothly from legacy systems to compliant frameworks.

G. Continuous Improvement

i. Implementation guidelines shall be reviewed after 3 years by the SDA.
ii. Feedback loops from monitoring, audits, and citizen engagement will inform revisions.
iii. Global best practices and new technologies (AI, blockchain, IoT, edge computing) will be progressively incorporated.

17 Monitoring & Audit

Monitoring and auditing are critical to ensuring that the State Data Governance Framework is effectively implemented, legally compliant, and aligned with the principles of transparency, accountability, and security. Continuous oversight mechanisms will build trust among citizens, improve departmental performance, and ensure data assets are used responsibly.

A. Monitoring Framework

The monitoring framework at different levels will be as follows:

i. **State Data Authority (SDA):**
   a. Tracks compliance with data classification, metadata standards, hosting protocols, and consent management.
   b. Provides alerts on anomalies or unauthorized activities.
ii. **Departmental Data Committees:**
   a. Maintain internal monitoring dashboards to log and audit all processing activity.
   b. Submit quarterly compliance reports to the SDA.
   c. Track departmental progress on cataloguing, classification, and data quality.
iii. **Performance Indicators:**
   a. Percentage of datasets catalogued and classified.
   b. Number of open datasets published.
   c. Compliance rate with metadata and interoperability standards.
   d. Incidents of breaches or unauthorized data access.

e. Citizen feedback and satisfaction on open data services.
f. Others as may be necessary.

B. Audit and Compliance Framework

This Data Governance Framework shall establish a two-tier audit mechanism to ensure continuous compliance, risk mitigation, and accountability in the processing of personal data by State departments.

Tier I – Internal Audit
All Data Fiduciaries shall conduct periodic internal audits, at least annually, in accordance with an audit framework, methodology, and reporting format prescribed by the State Data Authority (SDA). These audits shall assess compliance with applicable data protection obligations, SOPs, and security controls.

Tier II – Independent Statutory Audit
Departments or entities designated as Significant Data Fiduciaries (SDFs) shall be subject to periodic audits by a qualified and independently appointed Data Auditor. The audit report shall be submitted directly to the State Data Governance Council (SDGC) and, where required under applicable law, to the Data Protection Board of India.

The audit framework issued by the SDA shall adopt a **risk-based approach**, prescribing audit frequency, depth, and scope based on factors such as data sensitivity, scale of processing, and risk exposure.

C. Reporting Mechanisms

The following reporting mechanism will be followed:

i. **Quarterly Departmental Reports:** Submitted by Departmental Data Committees to the SDA.
ii. **Public Disclosure:** Non-sensitive audit findings and performance summaries to be published for public awareness, enhancing transparency.

D. Continuous Improvement

The lessons learnt from incident/audit and continuous improvement should be incorporated to the data governance framework:

i. Lessons from audits will be fed back into revisions to this data governance framework and implementation guidelines.
ii. Capacity-building workshops will address gaps identified during audits.
iii. Best practices will be shared across departments to improve compliance uniformly.

18 Legal Framework

The State Data Governance Framework is grounded in the broader legal and regulatory ecosystem that governs data protection, privacy, digital governance, and information security in India. Implementation of this framework shall strictly adhere to these frameworks, ensuring that

all data-related activities are compliant with existing laws and aligned with emerging legal mandates.

A. National Laws and Acts

The following central legislations form the core legal foundation for this framework:

i. Digital Personal Data Protection Act, 2023 (DPDP Act)
ii. Information Technology Act, 2000 (as amended in 2008)
iii. National Data Sharing and Accessibility Policy (NDSAP), 2012
iv. Right to Information Act, 2005 (RTI)
v. Public Records Act, 1993
vi. Evidence Act, 1872 (as amended for electronic evidence)

B. Sector-Specific Regulations

Implementation of the State Data Governance Framework must also be consistent with domain-specific frameworks, including but not limited to:

i. National Digital Health Mission (NDHM) / Ayushman Bharat Digital Mission
ii. UIDAI / Aadhaar Act, 2016 and Regulations
iii. RBI Guidelines & Payment Systems Laws
iv. Ministry of Road Transport and Highways (MoRTH) Guidelines
v. Geospatial Data Guidelines, 2021 (Department of Science & Technology, GoI)

19 International and Standards References

The data governance framework also suggests taking into account global best practices and industry standards for data standardization, including:

a) ISO/IEC Standards (27001, 27701, etc.)
b) Metadata Standards (Dublin Core, DCAT. ISO/IEC 11179 etc)
c) Adherence to relevant and current open standards for metadata and data.

In essence, this framework is not standalone but functions within the larger legal framework of India's digital governance regime. Compliance with these laws and guidelines ensures that the State Data Governance Framework is both legally enforceable and future ready.

Directorate of ICT & e-Governance
Department of Science & Technology
Government of Gujarat