



THE ASSAM GAZETTE

অসাধাৰণ

EXTRAORDINARY

প্ৰাপ্ত কৰ্তৃত্বৰ দ্বাৰা প্ৰকাশিত

PUBLISHED BY THE AUTHORITY

নং 259 দিশপুৰ, বুধবাৰ, 17 জুন, 2026, 27 জেঠ, 1948 (শক)

No. 259 Dispur, Wednesday, 17th June, 2026, 27th Jaistha, 1948 (S. E.)

GOVERNMENT OF ASSAM

ORDERS BY THE GOVERNOR

INFORMATION TECHNOLOGY DEPARTMENT

NOTIFICATION

The 16th June, 2026

No. IT.272131/380.- In supersession of the Assam State Data Policy, 2022, and to operationalise a State-wide data governance framework aligned with the Digital Personal Data Protection Act, 2023, and to enable secure, permissioned data sharing for improved governance and service delivery, the Governor of Assam is pleased to notify the **Assam State Data Policy, 2026**, appended to this Notification.

The Assam State Data Policy, 2026 shall come into force from the date of its publication in the Official Gazette.

The Government of Assam may amend the Policy from time to time, as deemed necessary.

K S GOPINATH NARAYAN,

Principal Secretary to the Government of Assam,
Information Technology Department.

Assam State Data Policy 2026

- | | |
|--------------|--|
| Introduction | <p>1. (1) Value potentials of data are widely recognized at all levels. Better use of reliable data can revolutionize the public sector, giving the means for efficient and transparent governance, more responsive service delivery, enabling citizens to make informed decisions, and innovation in sectors critical for societal transformation. With increased digitization and enhanced e-enabled engagements, the volume of data is also surging exponentially; however, the true potential of data in the government is yet to be realized fully. Even though large quantum of publicly funded data gets generated by various departments, organizations and institutions of the government, access to such data systems remains confined to individual departments in a largely disconnected manner. Common guidelines on what data can be shared, how to make data available for use within and across departments, protocols for making data available for external parties etc. are usually not well delineated impeding the emergence of a data-driven decision-making culture in the Government.</p> <p>(2) Recognizing the importance and potential value of data generated by the government departments, organizations, institutions and autonomous bodies for data-driven responsive governance, Government of Assam has pioneered data-driven governance for tackling pressing implementation challenges and achieving desired outcomes on high priority initiatives of the Government. Framing of the State Data Policy is one of the critical ingredients in this direction. The Assam State Data Policy (ASDP) seeks to define the rules of engagement with regards to all aspects of data management and governance, making optimal use of data for evidence-based decision making, and at the same time ensuring citizens' right to privacy which is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution.</p> <p>(3) The Assam State Data Policy provides the framework and guidelines for collection and collation of data, publishing open data, and secure access to non-open data to catalyze research and policy making by the departments, institutions and autonomous bodies of Assam Government; and sharing of data with bona fide external agencies collaborating with the government to strengthen policy processes and programme implementation.</p> |
| Vision | <p>2. (1) The Assam State Data Policy envisions to intrinsically transform Government of Assam's ability to harness cross-sectoral data generated with public resources to catalyze large scale social transformation by building digital and data capacity across the administrative hierarchy for improved evidence-based policy process, better implementation and monitoring of development and welfare programmes, and efficient delivery of citizen centric services.</p> <p>(2) This vision rests on a trusted data ecosystem that ensures responsible, secure and ethical use of data, and promotes data as a valuable asset for public good.</p> |
| Objectives | <p>3. (1) The Assam State Data Policy is framed with the objective of laying down the principles and direction on data accessibility in both human readable and machine-readable forms while safeguarding citizens' right to privacy, towards enabling data-driven governance with data derivatives serving as public good to</p> |

		enhance government efficiency, improve access to quality public services and delivery of citizen centric benefits, and help advance digital transformation.
		(2) The ASDP shall promote the responsible use of data as a strategic public asset, not only for government operations but also to enable research, innovation, and evidence-based decision-making, thereby contributing to Assam's overall growth strategy.
Scope and Applicability	4.	(1) The Assam State Data Policy provides the framework and guidelines for collection, collation and processing of data in machine readable format; classification and publishing of open data; secure and restricted access of non-open data across departments towards effective policy formulation and programme implementation; and secure permissioned access of anonymized/de-identified datasets to entities outside of government for bona fide research and analytical studies aimed at policy design and implementation. (2) The Assam State Data Policy shall be applicable to all data and information created, generated, collected, and archived by departments, institutions, organizations, autonomous bodies of Government of Assam, using public funds provided by the State or the Central Government, across all tiers of government. (3) This Policy will also apply to data that is recurring in nature and generated owing to automation of government processes and the results emerging out of these for delivery of services and benefits to citizens and businesses, as well as the legacy government data that is still available in non-machine-readable form within the State of Assam. (4) Government of Assam will proactively engage with the autonomous councils for adoption of Assam State Data Policy within their territorial jurisdiction.
Definitions	5.	(1) Aggregation: Refers to the process of creating higher level data by combining data across Data Principals so that it does not reveal any personally identifying information about Data Principals. Aggregation is a way of anonymizing data. (2) Anonymization: In relation to personal data, refers to the irreversible processes of transforming or converting personal data into a form through which a Data Principal cannot be identified even if the information is combined with other information, after reasonably considering factors such as time, cost and technology. (3) Data: A representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means. It covers all aspects of government functioning including G2G, G2B and G2C. (4) Data archive: The digital location where machine-readable data is stored, worked upon / analyzed, documented prior to a cut-off past date. (5) Data Custodian: The entity responsible for the safe custody, transport, storage, and preservation of data assets. For the purposes of this Policy, the Government of Assam is the overarching Data Custodian of all public data.

- (6) **Data Fiduciary:**
Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
- (7) **Data generation:**
Initial collection of data or subsequent addition of data to the same specification. This may be data specifically collected for a particular objective or may be a consequence of the authorized administrative processes of the Government.
- (8) **Data Principal:**
The individual to whom the personal data relates and where such individual is - (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.
- (9) **Data Processor:**
Any person who processes personal data on behalf of a Data Fiduciary. For the purpose of this policy, this includes any service provider, system integrator, or agency (Central or State) hosting or managing data infrastructure for a department.
- (10) **Data standards:**
Frameworks that define and embed data handling functions (e.g. data collection, management, transfer, integration, publication); and operate on data in a manner that complies with data format and data syntax specifications produced and maintained by standards bodies.
- (11) **Dataset:**
A distinct, discrete collection of data elements selected or extracted from a source system or database. It is a static or dynamic artifact prepared for a specific purpose, defined by a specific schema, and may differ in classification from its source system. A dataset also includes associated metadata describing its content, provenance, and usage to enable effective storage, analysis, sharing, publication, etc.
- (12) **De-identification or pseudo anonymization:**
Means the process by which identifiers from personal data may be removed, or masked, or replaced with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the Data Principal.
- (13) **Derived datasets:**
A dataset created by processing, transforming, or aggregating data from one or more source systems. Derived Datasets are generated to facilitate analysis, reporting, or sharing, and may have a different structure, classification, or level of detail from the source system. They are managed in accordance with applicable standards and governance policies to ensure accuracy, integrity, and usability.
- (14) **Information:**
Data embellished with a context, in other words, 'processed data.'
- (15) **A machine-readable format:**
It is a structured data format that computers and software applications can easily and automatically recognize, read and process (e.g. csv, json, xml, etc.).

(16) Metadata:

Data describing the structural, administrative, and descriptive characteristics of a dataset. It includes information on the source, origin, quality, and conditions of data generation, as well as the methods, classifications, and nomenclature used, to facilitate the discovery, traceability, and responsible reuse of data assets.

(17) Personal data:

Any data about an individual who is identifiable by or in relation to such data.

(18) Personally Identifiable Information:

Data about or relating to a Data Principal who is directly or indirectly identifiable, whether online or offline, or any combination of such features with any other information; and shall include any inference drawn from such data for the purpose of profiling.

(19) Shareable Dataset:

Structured collection of data elements identified and approved for access and use beyond the source system. Shareable datasets may be classified as Open (publicly accessible) or Permissioned (restricted access) and are curated to ensure that they can be safely shared while retaining analytical or operational value.

(20) Technical Custodian:

The entity designated to oversee the management and governance of public data systems. Its responsibilities include maintaining data platforms and infrastructure, enforcing data policies and standards, ensuring secure storage and controlled access to public data, enabling data sharing, and facilitating the effective and compliant use of data across government. For the purposes of this Policy, the Centre for Data Management (CDM) shall be the Technical Custodian of Public Data in Assam and shall ensure that all systems are secure, interoperable, and operate reliably in accordance with applicable policies and standards.

Guiding Principles

6. To realize the vision and achieve the objectives, the policy is anchored on the following guiding principles:

(1) Openness and Public Value:

Non-sensitive, anonymized, machine-readable datasets shall be openly accessible to promote transparency, innovation, and public benefit. Open data shall follow standards, metadata frameworks, and technical protocols enabling responsible reuse. The Government shall actively promote the use of open datasets to foster innovation, entrepreneurship, and AI-driven solution development, including through mechanisms such as hackathons, Grand Challenges, and collaboration with startups and university incubation centres.

(2) Privacy and Personal Data Protection:

Personal data shall be collected, processed, and shared only for lawful purposes, in compliance with the Digital Personal Data Protection Act, 2023, and relevant sectoral laws.

(3) Ethics, Fairness, and Equity:

Data use shall be ethical, non-discriminatory, and transparent, promoting equitable opportunities while safeguarding individual rights.

- (4) Transparency:
Data access, sharing, and release processes shall be documented, including provenance, transformations, and limitations on use.
- (5) Legal Compliance:
All data activities shall comply with applicable laws on privacy, security, confidentiality, and intellectual property while enabling beneficial use.
- (6) Intellectual Property and Responsible Reuse:
Proprietary or copyright-protected datasets shall not be released as open data. Open licensing, such as Creative Commons, shall be encouraged to support lawful reuse, innovation, and public benefit.
- (7) Interoperability and Standards:
Departments shall adopt common standards, metadata frameworks, and interoperable architectures to reduce fragmentation, duplication, and inefficiencies.
- (8) Data Quality and Usability:
Data shall be accurate, complete, timely, and maintained consistently. Metadata and quality checks shall support meaningful interpretation, accountability, and trust.
- (9) Data Security and Resilience:
Data and infrastructure shall be protected against unauthorized access, breaches, manipulation, or cyber threats, following national and state cyber security guidelines.
- (10) Accountability and Stewardship:
Clear responsibilities shall be defined for data governance. Departments and designated data stewards shall ensure quality, security, lawful use, and ethical handling of all data assets.
- (11) Sustainability:
Data governance initiatives, platforms, and open data efforts shall be supported through sustainable technical, operational, financial, and legal arrangements to ensure long-term continuity and value.

Data
Governance and
Management
Framework

7. To implement the principles above, the following data governance and management framework shall guide all departments and agencies:

- (1) Data Collection, Custodianship, and Sovereignty
 - (i) Collection of primary data shall predominantly be the responsibility of government departments and institutions mandated for policy process, programmatic implementation, and/or service delivery.
 - (ii) Data collection, irrespective of the primary data acquisition mechanisms (whether human-mediated, electronic, or via IoT devices), shall be ethical and strictly compliant with the Digital Personal Data Protection (DPDP) Act, 2023 and prevailing security legislations.
 - (iii) Rights and Custodianship:
In the case of personal data, rights shall vest in the Data Principal as defined under the DPDP Act, 2023, with the concerned Department, Institution, or Autonomous Body serving as the Data Fiduciary. For all data generated, collected, or processed using public funds, the Government of Assam shall be the sole Data Custodian. The Centre for

Data Management (CDM) shall serve as the Technical Custodian and central repository for these publicly funded digital data systems, ensuring secure storage, controlled access, interoperability, and efficient technical operations.

(iv) Data Sovereignty and Processors:

Any agency, partner, system integrator, or technology service provider (including Central Government agencies, State PSUs, or private vendors) hosting or processing data on behalf of the Government of Assam shall act strictly as a Data Processor. They shall have no ownership rights over such data or the derived datasets. All such Data Processors are mandated to provide raw data access, open APIs, or database dumps to the Data Fiduciary or the CDM upon request, without hindrance or delay, to ensure the sovereignty of the State over its own data assets.

(v) Digital-First Approach and Quality:

Wherever feasible, a digital-first approach to data collection shall be adopted. The digitization of legacy paper-based records shall be prioritized based on: (a) high-frequency public service delivery requirements, (b) inter-departmental dependencies, and (c) statutory obligations. Rigorous validation rules, input constraints, and automated quality checks must be applied to uphold the accuracy, completeness, and consistency of collected data.

(vi) Security and Standards:

Secure storage is paramount, requiring the use of encryption, robust access controls, and protected hosting environments to safeguard sensitive information. The CDM will establish and disseminate comprehensive standards, guidelines, and protocols governing the processes of data collection, validation, and storage, thereby ensuring uniformity and security across all state departments. Security safeguards shall be implemented in conformity with the reasonable security safeguards prescribed under Rule 6 of the Digital Personal Data Protection Rules, 2025, as amended from time to time. The CDM shall issue detailed compliance controls and standards through the Operational Guidelines.

(vii) Data Localisation and Hosting Safeguards:

Sensitive, personal, and non-shareable government datasets shall be hosted and processed only on State-controlled infrastructure (including the State Data Centre), MeitY-empanelled Cloud Service Providers, or other infrastructure approved by the Government of Assam, ensuring that such data is stored within Indian territory and subject to Indian law. Data Processors and service providers shall be contractually required to comply with applicable data residency and sovereignty conditions. The CDM shall notify the list of approved infrastructure and any dataset-category specific hosting requirements through the Operational Guidelines.

(2) Lawfulness of Processing

- (i) Strict compliance with the Digital Personal Data Protection (DPDP) Act, 2023 and all relevant sectoral laws are mandated to ensure all data activities are lawful and protective of individual rights.

- (ii) The ASDP offers operational guidance on key aspects such as governance, interoperability, data quality, institutional responsibilities, and data-sharing, while avoiding duplication of statutory provisions. To uphold these standards, the CDM is tasked with monitoring departmental practices and issuing necessary guidance to ensure ongoing compliance across all data-related operations.
 - (iii) Departments and the CDM shall ensure compliance with Rule 13 of the Digital Personal Data Protection Rules, 2025, including obligations relating to data retention, erasure, and the processing of children's data, as applicable. Detailed compliance procedures shall be prescribed in the Operational Guidelines.
- (3) Data Interoperability and Meta Data
 - (i) To ensure consistency and efficiency in data management across all departments, common standards and interoperable data elements need to be adopted. Comprehensive metadata catalogues will be maintained that clearly define datasets, specify ownership, indicate update frequency, and establish the source of truth.
 - (ii) The CDM will be responsible for maintaining and regularly updating the interoperability frameworks and guidelines, ensuring seamless data exchange and alignment with best practices.
- (4) Securing the Data System

To safeguard data assets and prevent unauthorized access or misuse, all departments must implement robust security standards in accordance with national and state guidelines. Regular audits should be conducted by CERT-In empanelled auditors to assess and strengthen security measures. The CDM will be responsible for issuing detailed administrative procedures and periodically reviewing departmental compliance, ensuring that data security remains a top priority across the organization.
- (5) Data Classification and Access

To facilitate responsible data sharing without compromising privacy or security, a clear distinction shall be made between Source Data Systems (live databases/applications) and Datasets (discrete artifacts extracted from sources). Departments shall classify all Datasets generated or derived by them according to the following structure:

 - (i) Open Access Data

Open Datasets are intended to be freely used, reused, and republished for lawful purposes without restrictions.

 - (a) Default Position: Data generated from public funding should, by default, be provided in machine-readable formats (e.g., CSV, JSON, XML) to facilitate transparency and innovation.
 - (b) Treatment of personal data: Source systems containing personal data cannot be Open Access. However, Derived Datasets extracted from such systems may be classified as Open Access provided they have undergone irreversible aggregation or anonymization (e.g., district-level health statistics derived from patient records) such that no specific Data Principal can be identified.

(ii) **Permissioned Access Data:**

Datasets accessible only to authorized agencies or individuals through a defined approval process. This category applies to data that is non-personal but restricted, or personal data required for specific lawful purposes. This category follows a Dual-Track Protocol:

(a) **Track A - Intra-Government Sharing (G2G):**

For statutory functions (e.g., beneficiary de duplication, fraud detection, service delivery), Permissioned Access datasets containing personal identifiers may be shared between government departments. This is subject to: Strict compliance with the DPDP Act, 2023 (lawful purpose), Adherence to Data Sovereignty principles, Use of secure data pipelines (APIs) and encryption. Anonymization is not mandatory for Track A if the specific statutory function requires personal identifiers.

(b) **Track B - External Sharing (Research & Innovation):**

For sharing with external entities (Universities, Think-Tanks, Development Partners, Private Sector), datasets must undergo strict anonymization, aggregation, or de-identification prior to sharing. No personally identifiable information shall be shared with external entities without the explicit, informed consent of the Data Principal or a specific statutory exemption.

(iii) **Non-Shareable Data:**

Data that is strictly confidential due to implications for national security, strategic interests, or statutory prohibitions (e.g., under the Aadhaar Act or RTI Act exemptions).

(a) **Scope:** This category includes highly sensitive raw intelligence, encryption keys, or un-redacted records where the risk of harm outweighs any public benefit.

(b) **Exception:** Even Non-Shareable data may be accessed by law enforcement agencies or competent authorities strictly in accordance with the procedure established by law (e.g., court orders).

(6) **Rules of Access to non-open Data:**

(i) Access to permissioned datasets shall be governed by the rules established by the CDM, considering factors such as sensitivity, anonymization, intended purpose, and eligibility for access.

(ii) Data should be shared exclusively through secure APIs or controlled environments, with direct database access strictly prohibited to maintain security and integrity.

(iii) Comprehensive data sharing agreements are required to clearly define permitted uses, retention periods, safeguards, and penalties for misuse. Cross-departmental analytics and bona fide research are encouraged provided due diligence is exercised to ensure compliance and responsible data handling.

- (iv) All access to permissioned datasets shall be purpose-limited, approval-based, and fully logged and auditable. Access shall be provided exclusively through secure APIs or controlled environments under a valid data-sharing agreement, and shall not extend beyond the scope of the approved purpose.

(7) Redressing Grievances of Data Principals:

All personal data grievances must be addressed in accordance with the procedures outlined in the DPDP Act, 2023. Each department is responsible for maintaining robust operational processes to manage such grievances effectively, while the CDM coordinates with appellate authorities to ensure proper resolution and compliance across the organization.

(8) Digital Data Registries:

The CDM will facilitate the development of centralized, authoritative registers that serve as the single source of truth for major datasets across departments. These registers must be maintained with a high degree of accuracy, regularly updated, and fully synchronized with departmental workflows to ensure data integrity and reliability throughout the organization.

(9) State Data Catalogue:

The CDM in collaboration with all departments, will maintain a comprehensive State Data Catalogue to facilitate the discoverability and access of all public datasets, encompassing both open and permissioned data. This catalogue will include essential metadata, clearly defined access conditions, applicable standards, and guidance to ensure the lawful and responsible use of data assets.

State Data
Governance
Architecture

8. (1) State Data Management Steering Committee (SDMSC):

- (i) The SDMSC will coordinate and monitor the implementation of Assam State Data Policy through close collaboration with all state government departments and agencies.
- (ii) SDMSC will include Senior-most Secretaries of IT, Finance, Revenue, ARTPPG, P&RD, Urban Development, Health, Education, Forest and other departments dealing with large datasets. The SDMSC will be headed by the Chief Secretary and the CDO will be the Member Secretary. The composition of the Committee may be reviewed and revised as and when needed.
- (iii) SDMSC shall function as the apex decision making authority on all issues relating to data governance standards and benchmarks in the State. The SDMSC shall have the following responsibilities:—
 - (a) SDMSC will convene biannually or as and when needed to assess the implementation and compliance of the data policy.
 - (b) SDMSC will convene biannually or as and when needed to assess the implementation and compliance of the data policy.
 - (c) Approve rules, guidelines, and standards for data governance and management.
 - (d) Define and notify what constitutes as master data which shall be standardized across all the departments.

- (e) Approve the state-level data classification framework (Open, Permissioned, Restricted, etc.).
 - (f) Define and maintain a negative list (or restricted data list) specifying datasets or data elements that cannot be shared or published.
 - (g) Promote and facilitate the sharing of data and information among various departments & other users.
- (2) Centre for Data Management (CDM):
- (i) The Government of Assam shall notify the CDM, operating as a specialized vertical within the AITEC & CSD Society, as the nodal agency for facilitating and enforcing the implementation of this Policy. The CDM shall function under the administrative control of the IT Department.
 - (ii) The CDM shall be empowered to formulate operational guidelines, standards, and protocols needed to ensure adequate implementation of the ASDP; issue notifications, operational clarifications, advisories, and code of practices for nuanced interpretations of the Policy and to promote good practices; and recommend amendments to the Policy for Cabinet Approval, as and when needed.
 - (iii) All departments shall provide CDM with secure access to their data assets, including personal data in accordance with the DPDP Act, 2023, to enable CDM to support data quality, harmonization, enterprise-wide data governance and management, and to prepare derived datasets for authorized use.
 - (iv) Mandate:

Towards realization of the vision and objectives of ASDP the CDM shall have the following mandate to,—

 - (a) Data Strategy and Governance:

Implement and enforce the Assam State Data Policy across all government departments; Ensure citizen engagement creating awareness regarding data sharing, transparency and trust; Coordinate with national central bodies like MEITY and the Data Protection Board of India; Ensure collection, interpretation and recording of data in accordance with the ASDP standards.
 - (b) Data Management and quality:

Enable cross-department data sharing, use, and analytics initiatives through digital transformation, shared infrastructure, and capacity building; Build and maintain a state data catalogue which facilitates discoverability and access to data through a single point of entry; Oversee master data and metadata management, data management, business glossary development, and development of other enterprise-wide artifacts that enable effective use of data.
 - (c) Data Analytics and Insights:

Drive data analytics initiatives to extract valuable insights and support data-driven decision-making;

Collaborate with stakeholders to help them identify key performance indicators and develop dashboards and reports for monitoring and reporting.

(d) Data Privacy and Security:

Make information appropriately accessible within a protected and trusted environment subject to access, security, and privacy rules; periodically review data policy compliance by departments, institutions, organizations and autonomous bodies covered under the ASDP; Approve restricted data usage ensuring privacy and legal safeguards; Ensure compliance with data protection laws and other data regulations issued at the federal and state level; Collaborate with the officials responsible for data privacy and any state specific protocols necessary for the implementation of data security and protection; Monitor and respond to personal data breaches or misuse; Facilitate the resolution of citizen grievances related to data misuse and privacy violations.

(e) Data Innovation and Technology:

Monitor technological developments and practices so that the provisions of ASDP could be adapted in tune with technological advancements and emerging digitalization practices; Promote research and innovation in data-driven governance and emerging technologies; With relevant departments, identify transformative data projects with significant potential to improve efficiency and productivity and/or provide new insights into the performance of government policies and schemes.

(f) Stakeholder Collaboration:

Assign Data Stewards to support the Data Officers in implementing the ASDP; Provide technical and policy support to departments on data standards and practices; Train and support Departmental Data Officers in data handling and compliance; Collaborate with various departments and business units to understand their data needs and align data initiatives with organizational objectives; Educate and promote data awareness, data protection and security and literacy within the organization; Create user groups to capture and align data-use with user demand; Leverage the strategic partnerships of AITEC&CSD Society (e.g. with research orgs, think tanks, universities); Perform other related functions as may be prescribed by government from time to time.

(v) CDM Structure:

The Center for Data Management will be established under the AITEC&CSD Society. The CDM will have the following verticals. Each vertical will be headed by a Lead, reporting to the CDO, and will be supported by a team of specialists having relevant skills and experience.

(a) Policy, Guidelines and Standards:

This unit is responsible for setting data governance policies and procedures to ensure responsible and

ethical data use. It will establish data policy for the entire data lifecycle and set out framework for standards across different domains including geospatial, statistical, metadata, data quality, and API standards.

(b) Data Management, Analytics and AI:

This unit is responsible for managing all public data including collecting, storing, and organizing data in ways that ensure its integrity, validity, and availability. This entails developing and maintaining systems to catalogue and access data, making it easier to retrieve, manage and use information.

(c) Data Security and Compliance:

Ensure compliance with all relevant regulations and statutes related to data protection and privacy. Its task involves ensuring the security of data by implementing appropriate guidelines and standards, and safeguards. Manage grievance redress mechanism of all data related issues.

(d) Enablement, Communication and user outreach:

Strengthens institutional capacity by training government personnel, fostering data literacy, partnering with research and academic institutions, and promoting innovation and responsible data use across the state. Conduct periodic user consultations to ensure data needs for policy (and wider user base) are being met.

(e) Digital Transformation:

This unit will develop and maintain the data architecture, tools and platforms to support the objectives of the CDM and enable the various stages of the data lifecycle from collection, management, integration and dissemination of data. It will embed data standards and ensure that the principles of the data policy are integrated early in the design and development of all platforms and tools.

The CDO may appoint consultants and solicit services of relevant experts considered necessary for the effective discharge of CDM mandates.

(vi) Chief Data Officer (CDO)

The Project Director, AITEC&CSD Society will be the ex-officio CDO of Assam and will be the head of the CDM. The CDO will have appropriate administrative and financial authority, as well as budgetary provisions for taking all operational level decisions emanating from the ASDP. The CDO shall be responsible for day-to-day implementation of the State Data Policy. The CDO shall be responsible for the following:—

- (a) Lead the implementation of the Assam State Data Policy (ASDP) across all departments and ensure statewide compliance;
- (b) Oversee state-wide data governance, including data standards, metadata, master data management, and the State Data Catalog;

- (c) Drive cross-department data sharing and analytics, enabling evidence-based decision-making and improved service delivery;
 - (d) Ensure robust data privacy, security, and regulatory compliance, including oversight of restricted data access, breach response and grievance resolution;
 - (e) Promote data innovation, emerging technologies, and transformative data projects across government departments;
 - (f) Provide policy, technical, and capacity-building support to Departmental Data Officers, Data Stewards and departmental teams;
 - (g) Lead stakeholder engagement and citizen awareness efforts on data sharing, transparency, and privacy;
 - (h) Monitor ASDP implementation progress and submit mandated compliance reports to the SDMSC;
 - (i) Provide strategic leadership to the CDM, ensuring efficient operations, collaboration, and a culture of responsible data use;
 - (j) Build, lead and maintain a high-performing, multidisciplinary data team, including data scientists, engineers, analysts, and functional data governance officers;
 - (k) Establish the foundational structure, workflows, and operating norms for the CDM, ensuring clarity of roles, responsibilities, and accountability;
 - (l) Chair the DIDC to help collect, collate, process and publish data in line with ASDP;
 - (m) Serve as the Member Secretary of the SDMSC, ensuring the committee meets regularly, agendas capture all relevant issues, and all reporting, documentation, and follow-up actions are completed in a timely manner.
- (3) Data Inter-Departmental Committee (DIDC)
- (i) The DIDC shall be constituted with all the Departmental Data Officers, under the Chairmanship of the CDO. The DIDC shall serve as the principal coordinating body for data governance across the Government of Assam.
 - (ii) The DIDC shall:
 - (a) Coordinate data governance across departments and oversee adoption of standards, policies, and common practices.
 - (b) Facilitate safe data sharing for operational, analytical, and public-good use while ensuring compliance with legal and privacy requirements.
 - (c) Improve data quality and metadata by supporting departments in maintaining accurate, timely, and interoperable datasets.
 - (d) Strengthen evidence-based decision-making by enabling cross-departmental analytics and identifying priority use cases.
 - (e) Review compliance with the ASDP and address

issues, risks, or data-related grievances raised by departments or users.

- (f) Support partnerships and research access, ensuring that any external data-sharing adheres to approved safeguards and agreements.
- (iii) To carry out its functions effectively, the DIDC may form focused working groups on Open Data, Data Quality, Analytics, Compliance, and Partnerships, as needed.
- (iv) The DIDC shall be supported by technical and analytical professionals from the CDM and relevant departments.
- (4) Departmental Data Officers
 - (i) Departments/Institutions/Autonomous Bodies under Government of Assam would nominate a Data Officer (DO) at a senior level, at least Joint Secretary or above and preferably having experience of working on digital data management/governance.
 - (ii) The Departmental Data Officer shall be responsible for supporting the implementation of the ASDP in their respective departments and carrying out the decisions of the SDMSC and DIDC. The CDM will assign Data Stewards to provide technical assistance, guidance, and training to Department Data Officers.
 - (iii) Mandate for Data Discovery and Dataset Definition:

To ensure that the State's data assets are effectively catalogued and utilized, the departmental DO shall be responsible for the following time-bound activities:

 - (a) Annual Data Asset Inventory:

The DO shall develop and maintain a mandatory Data Inventory identifying all digital data assets (including databases, applications, registries, and dashboard back-ends) held by the Department. This inventory shall be maintained in a Data Asset Register as per the format prescribed by the CDM and updated at least annually. Data Stewards will assist the DO in mapping source systems and drafting the inventory.
 - (b) Definition of Shareable Datasets:

Based on the Data Asset Register, the DO, in consultation with the CDM and with support from assigned Data Stewards, shall identify and define specific 'Shareable Datasets' that can be extracted or derived from the source systems. The DO shall distinguish between the Source System (which may be restricted) and the Derived Dataset (which may be classified as Open or Permissioned).
 - (c) Mandatory Metadata Publishing:

Regardless of whether the actual data is shared immediately, the publication of metadata is mandatory. The DO must publish the Metadata for all identified datasets in the State Data Catalogue within 30 days of their identification in the Data Inventory.

Training and
Skill
Development

- 9. (1) The CDM shall assess relevant training needs, develop comprehensive training plans, and implement regular programs for skill development and capacity building of all government personnel. Special emphasis will be placed on those involved in

- data collection, processing, management, and use, ensuring they are equipped with up-to-date technical knowledge and best practices required for the successful implementation of the ASDP and effective evidence-based decision making.
- (2) In addition to regular training and upskilling of government manpower, the CDM will also build data capacity across the broader data community, actively fostering collaboration, knowledge exchange, and professional development opportunities to build a vibrant, skilled, and engaged data ecosystem within Assam. Dedicated initiatives will be undertaken to connect data practitioners, researchers, and innovators, enabling the growth of a strong data community that supports evidence-based governance and drives continuous improvement in data-driven decision making.
- Budgetary Provisions** 10. Adequate budget provisioning will be made by Government of Assam to enable CDM to implement the ASDP.
- Policy Implementation Support and Compliance Monitoring** 11. (1) Detailed Operational Guidelines for ASDP implementation will be notified by the CDM with approval of SDMSC; and will be updated on need basis. The Operational Guideline shall include the technology and standards for data collection, processing, storage and sharing; criteria and mechanism for restricted access data sharing; suggested format for publishing Metadata catalogues; model data sharing and licensing frameworks. The Operational Guidelines will be updated from time to time as needed.
- (2) Policy compliance monitoring will be conducted by the CDM in collaboration with the departments/agencies on a bi-annual basis (every six months). The compliance reports will be submitted to the SDMSC for review and necessary guidance.
- Benefits of State Data Policy** 12. (1) Equity of data-access:
The ASDP practice of open access data will ensure better access to all bona fide users.
- (2) Maximizing data use:
Access to government-owned data will enable the more extensive use of the information to deliver services and facilities in an efficient and transparent manner.
- (3) Maximized integration:
Adoption of common standards and best practices across various datasets and MIS would facilitate the integration of individual datasets.
- (4) Interoperability to avoid duplication:
By facilitating the sharing of required data across departments, the need for separate bodies to collect the same data will be minimized. This will result in significant time and cost-saving in data collection and also eliciting a rounded perspective on the performance of government initiatives and schemes.
- (5) Better decision making:
Availability of data will enable data-driven decision making along with avenues and platforms for monitoring, reporting and planning.
- (6) Better tracking for policy implementation:
Real-time availability of data will allow and open pathways for live tracking of policy implementation and impact, especially for welfare schemes.

-
- | | | |
|---|-----|--|
| | (7) | Enhanced and efficient delivery of services:
Data sharing and interoperability through this policy will be instrumental in reducing leakages and plugging loopholes in the delivery of welfare services. |
| Period of
Validity of State
Data Policy | 13. | (1) The Assam State Data Policy in its present form will remain valid till any further revisions are approved by the cabinet.
(2) Upon notification, this Policy shall supersede the Assam State Data Policy, 2022. All actions taken under the previous policy shall be deemed to have been taken under this Policy. |