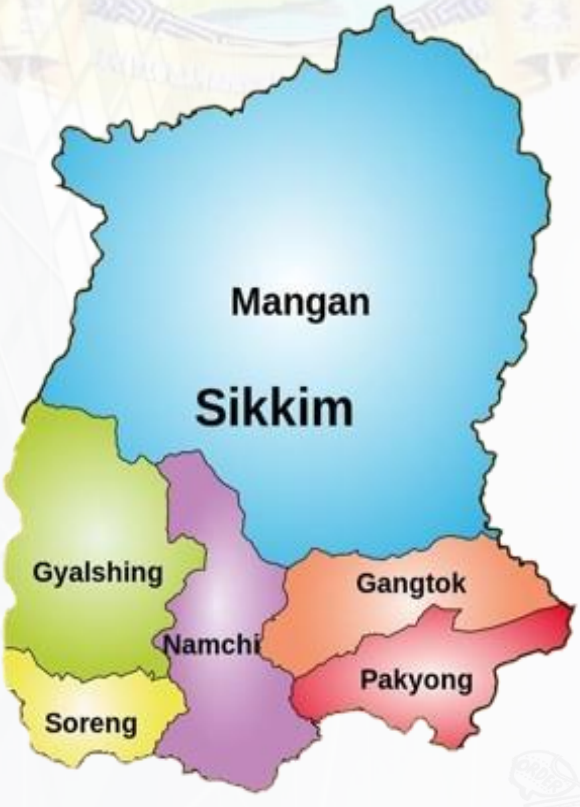
SIKKIM STATE DATA POLICY - 2025

GOVERNMENT OF SIKKIM



CONTENTS

Glossary of Terms

Abbreviation	Definition
AI	Artificial Intelligence
CDO	Chief Data Officer
CIA	Confidentiality Integrity and Availability
DEPA	Data Empowerment and Protection Architecture
DPDP	Digital Personal Data Protection
DPIV	Data Protection Impact Verification
DPO	Data Protection Officer
DR	Disaster Recovery
DESME	Directorate of Economic Statistics & Monitoring and Evaluation
ETL	Extract, Transform, Load
IT	Information Technology
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IPC	Indian Penal Code
IPR	Intellectual Property Rights
IoT	Internet of Things
MDM	Master Data Management
ML	Machine Learning
MIS	Management Information System
NDSAP	National Data Sharing and Accessibility Policy
NDCP	National Digital Communications Policy
NGO	Non-Governmental Organization
SSDP	Sikkim State Data Policy
SSDGTAC	Sikkim State Data Governance and Technical Advisory Committee
PSUs	Public Sector Undertakings
RTI	Right to Information
SDC	State Data Center
SDSC	State Data Steering Committee
SIEM	Security Information and Event Management
TRAI	Telecom Regulatory Authority of India

1 Preamble

In promoting efficient governance, transparency and accessible service delivery, reliable data is essential. Sikkim is digitizing its data infrastructure to create a strong framework for collecting, sharing, storing, and using data. Recognizing the value of data from Government departments, organizations, and institutions, the Sikkim State Data Policy 2025 (SSDP) provides comprehensive guidelines for data management. The policy ensures citizen privacy while effectively using data for evidence-based decision-making, thereby promoting informed governance.

The data policy aims to streamline the accessibility and sharing of Government-owned data. It provides open access to data in a format that supports sustainable governance, inclusive planning, effective implementation, and monitoring of development programs. SSDP prioritizes principles such as non-redundancy, openness, flexibility, interoperability, quality, efficiency, accountability, Intellectual Property Rights (IPR), and the rights to privacy and information.

Given the substantial amount of data used daily by Government, especially for providing welfare benefits, the state's data policy sets guidelines for storing and sharing various types of government-held data. This majorly includes personal, transactional, institutional, and procedural data. The policy promotes data interoperability to streamline processes, minimize redundant data entry, facilitate data sharing across departments and improve service delivery by addressing potential leaks and vulnerabilities.

A key element of Data Policy is 'Governance of Data,' which promotes the availability, quality, and security of departmental data through various standards and processes. The main objective of data governance is to maintain high-quality data that is transparent, secure, and easily accessible for public and departmental transactions.

1.1 Guiding Principles

To ensure effective data sharing and accessibility benefits for citizens and to empower departments improve service delivery frameworks using meaningful datasets, the SSDP is based on specific core principles. These principles include:

1.1.1 Open Data Accessibility

This principle sets the groundwork for smooth data sharing while preserving its intended use and value. Whenever possible and practical, promoting openness for data should be a priority, ensuring transparency and accessibility across all datasets.

1.1.2 Transparency

SSDP aims to ensure transparent access to Government data that is open, with clear tracing of sources and disclosure of any changes made. Regular reporting on data transparency will include updates, usage statistics, and feedback from stakeholders. Compliance with the policy will be enforced and monitored through procedures for reporting and resolving disputes.

1.1.3 Information Privacy

SSDP places utmost importance on Information Privacy, emphasizing the protection of personal data to prevent identity information from being disclosed. This principle requires safeguarding individuals' and groups' privacy rights, ensuring their data is kept confidential and secure. It mandates adherence to key principles such as obtaining consent, implementing strong data security measures, and clearly defining the responsibilities of data controllers and fiduciaries. Transparency, accountability, and the preservation of citizens' privacy rights are top priorities in all data-related activities under SSDP.

1.1.4 Ethical Conduct and Equality

In SSDP, it is crucial to highlight the importance of following moral standards and ensuring fairness in all data-related activities. This principle requires that data handling practices uphold ethical considerations such as respecting privacy, providing fair access, avoiding harm to individuals or society, promoting public good, and benefiting society equally. It mandates transparency, integrity, and impartiality in collecting, processing, and using data. SSDP must emphasize the commitment to ethical behavior, including non-discrimination or bias against any group or individual, allowing individuals to correct inaccuracies in their data, empowering users, and ensuring that data practices prioritize honesty, fairness, and inclusivity for all stakeholders.

1.1.5 Data Quality

SSDP focuses on accuracy, completeness, and reliability of data throughout its lifecycle and implement measures such as validation, verification, and data quality assurance processes. These steps are crucial for verifying the correctness and integrity of data at every stage of its existence.

1.1.6 Data Security

This principle aims to improve data protection by implementing safeguards against unauthorized access, disclosure, or misuse. This includes establishment of procedures to respond to data breaches, incidents, or security vulnerabilities to minimize harm and reduce risks to individuals and stakeholders.

1.1.7 Legal Conformity

SSDP adheres to relevant laws, including those at central and state levels that govern information protection, data security, privacy and remove legal barriers that hinder institutions and individuals from using data for the public good. SSDP aims to encourage the usage of data in ways that benefit society, by actively eliminating obstacles and respecting legal requirements.

1.1.8 Data Usability

This principle specifies allowed usage of data and also specify restrictions on data processing activities to ensure that data is used only for legal and legitimate purposes, preventing unauthorized access, misuse, or exploitation of data assets.

2 Definitions

2.1 Data

Data means 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.

2.2 Information

Information means 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.

2.3 Data Set

Dataset means a structured collection of data organized and stored together for analysis or processing.

2.4 Data Generation

Data Generation means an initial collection of data or subsequent addition of data to the same specification. It may be categorized into primary, satellite and aerial data collection by designated agencies and secondary data collection under the same specification (refers to modification or addition to the primary/initial data sets) through ground survey/data acquisition. This also covers non-human data collection via drones, bots, and other emerging Internet of Things (IoT) devices.

2.5 Data Catalog

Data Catalog means a collection of datasets under the same domain or sector.

2.6 Data Consumer

Data Consumer means an individual or organization that uses departmental data for decision-making, policy formulation, research or other meaningful purposes.

2.7 Data Archive

Data Archive means a secured storage system where machine-readable data after a cut-off date are stored, acquired, documented for long-term preservation, and distributed to others for further analysis and consumption. Retention policies and criteria for archiving data should be defined.

2.8 Consent Manager

Consent Manager means a person registered with the Data Protection Board of India, who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent and interoperable platform.

2.9 Data Fiduciary

Data Fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing personal data.

2.10 Data Principal

This refers to an individual to whom a personal data relates

Also, where such individual is:

- A child and also includes the parents or lawful guardian of that child.
- A person with disability and also includes her lawful guardian, acting on her behalf.

2.11 Data Coordinator

Data Coordinator means an individual assigned at department level who will assist the Chief Data Officer (CDO) to aggregate data demand from various channels and support initiatives for sensitizing department employees on the importance of data.

2.12 Data Steward

Data Steward means an individual who is responsible for the practice of ensuring that an organization's data is accessible, trustworthy, usable, and secure. A Data Steward oversees every stage of the data lifecycle: creation, storage, usage, archiving, and destruction of the data in accordance with organization's established data governance principles for promoting data quality and health.

2.13 Data Owner

Data Owner means an entity responsible for the overall management, access control, and protection of specific data within an organization.

2.14 Data Custodian

Data Custodian means an individual who oversees the storage, aggregation and usage of data sets.

2.15 Personal Data

Personal Data means any data about an individual who is identifiable by or in relation to such data. It refers to any information that can be used to identify an individual, such as names, addresses, email addresses, phone numbers etc. It encompasses both direct identifiers and indirect identifiers that, when combined, can reveal someone's identity.

2.16 Sensitive Data

Sensitive Data means personal data that requires extra protection because it can cause harm, discrimination, or privacy violations if misused. This includes details like health records, financial information, business information, intellectual property, classified government documents or personal identifiers such as voters id, aadhar number etc.

2.17 Sensitive Personal Data

Sensitive Personal Data means sensitive data having personal information about individuals such as passwords, biometric data, official identifiers, data processed under contractual agreements, health information, caste or tribe, religious or political belief or affiliation, genetic data.

2.18 Spatial/ Geo-Spatial Data

Spatial Data or Geospatial Data means data about physical objects that can be represented by numerical values within a geographic coordinate system. This type of data is geographically referenced, allowing for identification of the object's location along with its geographic position and attributes.

2.19 Sensitive Spatial/ Geo-Spatial Data

Sensitive Spatial or Geospatial Data means location data that, if disclosed or misused, could jeopardize privacy, security, or safety. This could include precise details about where individuals live and work, critical infrastructure like power plants and transportation networks, environmentally fragile areas, military and defense installations, and health and emergency service facilities. Safeguarding this data is essential to prevent potential risks to individuals, communities, and national security.

2.20 Sharable and Non-sharable Data

Shareable Data means data that are non-confidential and non-sensitive, meaning they do not include sensitive personal data, proprietary business details, or any other confidential elements requiring restricted access and can be shared openly with public. This data is often used for purposes such as transparency, research, or public information.

Non-shareable Data means data that are highly confidential and sensitive and access to such data is only permitted after following a specified process of registration and authorization.

2.21 Open Data Access

Open Access Data means data which may also be contributed by the public which should be easily accessible in a timely manner, should be user-friendly, and web-based, without requiring registration or authorization processes.

2.22 Registered Data Access

Registered Access Data means secured data that is kept safe and accessible only to registered users. This may include username, password, details provided during registration (such as name and email), records of usage of a service, and permissions granted.

2.23 Restricted Data Access

Registered Access Data means data that is available only to authorized users or entities. Access to this data is restricted to individuals or organizations who have undergone a specific process of registration, authentication, or approval set forth by the data policy/organization policy. This measure ensures that sensitive or confidential information is protected from unauthorized access or misuse, promoting data security and privacy within the framework of policy.

2.24 Internet of Things (IoT) Data

IoT Data means data collected from everyday objects connected to the internet, enabling them to communicate with each other. This data includes measurements such as temperature, location, or movement, which can be valuable for Government purposes.

2.25 Metadata

Metadata means as information about data, detailing its source, creation time, location, and conditions. It informs users about the who, when, what, where, why, and how of data generation. Metadata includes structural details like data and dataset definitions, administrative information, processing and audit trail data, descriptive elements, time series, and statistical features.

2.26 Master Data

Master Data means core data that does not change often and is used across many parts of a business or organization. Master data helps to ensure accuracy and consistency across different systems and operations.

2.27 Transactional Data

Transactional Data means data from actions like financial dealings or service interactions that also include timestamps and descriptions. Businesses and organizations analyze transactional data to understand their operations, customer behavior, and financial performance better.

2.28 Registry Data

Registry Data means a collection of real-time data stored in centralized systems, tracking details about individuals, organizations, or objects.

2.29 Directory Data

Directory Data means contact-related data about individuals or organizations. This may include names, addresses, phone numbers, email IDs, job titles, and organizational affiliations. In the context of a data policy, directory data represents data collected, stored, and used for maintaining contact and communication within an organization or among different entities.

2.30 Aggregated Data

Aggregated Data means summarized data compiled from various sources to provide an overall view while safeguarding privacy.

2.31 As on Date Data

As on Date Data means data that is considered accurate and up to date as of a specific date. It indicates point in time up to which the data is verified, ensuring that the data reflects most current and valid information available at that moment.

2.32 Incremental Data

Incremental Data means new or updated data added since the last data collection or processing. It involves handling only the changes rather than reprocessing the entire dataset each time.

3 SSDP 2025: Mission, Vision, Objectives and Benefits

3.1 Mission and Vision

Being a spearhead in leveraging technology for effective governance and to enhance transparency, accessibility, and efficiency in administration, the state of Sikkim is committed to create a framework that encourages the sharing, integration, and efficient utilization of high-quality governance data, while ensuring privacy, security, and adherence to ethical standards.

Mission:

Develop and adopt the SSDP to protect citizen privacy, and standardize the process of digitization, storage, and sharing of data within different departments of the state. This will also facilitate the sharing of data in the public domain to enable effective and transparent governance.

This initiative seeks to enhance the accessibility, security, and quality of data across Government departments and associated bodies.

By establishing clear guidelines and protocols, the policy aims to facilitate transformation in service delivery and processes for adopting policies.

Moreover, it aims to align with other standardized data policies in place to be recognized as best practices for addressing the unique data driven challenges and opportunities in the state of Sikkim. The policy also aims to implement capacity-building initiatives to equip government officials with the necessary skills and knowledge to effectively manage and utilize data resources.

Vision:

SSDP aims to fundamentally change how the Government of Sikkim uses publicly collected data from various sectors to drive change across society. This will be achieved by enhancing digital skills and data management capacities at all levels of administration to enable evidence-based policymaking, improve implementation and monitoring of welfare programs, and ensure efficient delivery of services for citizens.

The policy envisions a comprehensive framework for data governance that establishes clear standards and responsibilities for data management, ensures data security and privacy, and promotes data sharing with a commitment to transparency and confidentiality. It also emphasizes capacity building in emerging technologies, development of robust data infrastructure, and ethical use of data, all supported by a regulatory and legal framework that aligns with national and international best practices.

3.2 Objectives

The core objective of the policy is to enable the efficient use of data that the Government of Sikkim collects, generates, stores, and manages. It aims to provide a framework for the proactive disclosure of government data by different departments for the benefit of the residents of the state of Sikkim.

The data policy shall help the government streamline the processes of data governance, including data security, data collection, data sharing, data storage, and the maintenance of high-quality data.

The key objectives of the policy are to:

Minimize errors of inclusion and exclusion in service delivery: Data systems to proactively identify beneficiaries of Government programs as well as remove fraudulent and unnecessary beneficiary records that lead to leakages in service delivery.

Minimize redundancy and duplicity: Redundancy and duplicity in data collection shall be removed by data integration and rationalization within each department. Data minimization for privacy also help towards non redundancy.

Improve public administration: Government resources shall be skillful on data security, quality, documentation etc. to support in improving public administration.

Maintain Transparency: Sharing data between departments and with other government institutions or the public can enhance transparency in government processes.

Maximize data analysis and interpretation: Support enabling data interoperability, standardization, quality, and regulated access while ensuring privacy and data security.

3.3 Benefits from the Policy

3.3.1 Benefit to Government

Improved Governance, Data Quality and Transparency

The quality of data will be enhanced through the implementation of data standards and guidelines. Additionally, by standardizing the collection, processing, and sharing of data, the policy will improve the delivery of public services and make processes more transparent and accountable.

Economic Growth

Economic development shall happen by adopting data policy by all departments of the state. Factors such as data-driven decision making, innovative initiatives, and reduced corruption through transparent access to necessary data will significantly contribute to the state's growth.

Furthermore, transparent data practices can make Sikkim more appealing to investors. When investors have access to reliable data, it can lead to improvements in the state's economy, infrastructure, and regulatory environment.

Effective Disaster Management and Response

The Data Policy will facilitate the collection and sharing of geospatial and environmental data, which are crucial for disaster management and response efforts. Effective use of this data can save lives and reduce economic losses. It will enhance Sikkim's capacity to forecast, respond to, and recover from natural disasters.

Information on Data Ownership

Departments within the Government of Sikkim will have clear ownership and defined responsibilities for their data. To support this, each department is encouraged to develop a detailed catalog or metadata database. This will allow users to easily identify the officials responsible for managing the department's key data.

Encouraging Data de-Duplication or avoiding data redundancy

Data is often stored in multiple places within a department by mistake or on purpose. This can happen during complex work or to keep data safe. SSDP will help to remove these extra copies through the process of data de-duplication. This will make data more accurate, smaller databases, and minimize the cost on data management.

Maximize Usage of Data

Respective departments will provide high-quality metadata in standardized, machine-readable formats, making it easy for users to comprehend the context, source, and limitations of the data sets. This approach will facilitate the accurate interpretation and utilization of the data.

Better Access and Decision-Making

The policy will support the sharing of open and transparent data, ensuring that authentic users have access to the prepared metadata. This will enable decision-making to be more straightforward and efficient, based on the availability and accessibility of data for tasks across different departments.

3.3.2 Benefit to Communities

Strengthening Security and Protection of Privacy Rights

The policy will ensure the security and responsible use of citizens' personal information, adhering to privacy standards and safeguarding against breaches without compromise. Additionally, the policy will

protect citizens' privacy rights through a comprehensive regulatory and legal framework that governs the collection, sharing, security, storage, and maintenance of high-quality data.

Enhanced Public Services

The policy will pave the way for the creation of smarter and more responsive public services by ensuring that all citizens, especially those from marginalized or underserved communities, have access to information.

Social Awareness

The policy will enhance awareness and careful handling of public data across all departments. It will also educate the public on how to access and utilize non-restricted information for official purposes.

Transparency and Accountability

Providing public access to non-sensitive government data promotes transparency and enables citizens to hold public-facing departments accountable. This openness is fostered by the disclosure of information, allowing citizens and third parties to use the data.

3.3.3 Benefit to Researchers

Research and Development

Having a clear framework for data usage allows researchers to access valuable information for their studies. Being able to tap into a vast repository of data will aid academic research efforts.

3.3.4 Benefit to Entrepreneurs

Encourage Digital Ecosystem

A robust data policy will create a favorable and lasting environment for startups and digital businesses, fostering entrepreneurship throughout the state.

Support in Generation of Employment

The policy will be instrumental in supporting job creation. The data-driven insights produced by various departments will facilitate the gathering, analysis, and sharing of employment-related data, which will be advantageous for job seekers.

4
Scope and Applicability

The scope and applicability of this Data Policy are defined in adherence to Section 2(h) of the Right to Information Act, 2005, and Digital Personal Data Protection (DPDP) Act, 2023.

The policy is closely applicable to all below mentioned public authorities defined in Section 2(h) of the Right to Information Act, 2005 where "public authority" means any authority or body, or institution of self-government established or constituted:

- by or under the Constitution
- by any other law made by Parliament
- by any other law made by State Legislature
- by notification issued or order made by the appropriate Government and includes any–
  (i) body owned, controlled, or substantially financed.
  (ii) non-Government organization substantially financed, directly or indirectly by funds provided by the appropriate Government.

This policy applies to all state government departments, agencies, and entities that collect, process, store, and manage data of multiple types. This policy also applies to those data being managed by private entities which are being shared with government as per specific need.

The policy also aims to safeguard individuals' privacy rights while promoting data security and compliance with legal and regulatory requirements as mandated by the DPDP Act, 2023.

5 Core Components of Data Policy

5.1 Core Data Principles

The Data Policy shall be guided by the following core principles:

- Data should be treated as a strategic asset that forms an important component of the business value chain.
- Data should be unambiguous and coherent to be usable by stakeholders outside of the data source.
- All departments should ensure compliance over policies and guidelines relevant to the data ecosystem. These may include policies implemented at Centre, State, and Departmental level.
- Clear accountability and ownership of data should be maintained throughout its existence, from collection to disposal.
- Data quality must be ensured and upheld consistently to ensure future use in sustainable and trustworthy repositories.
- There should be transparency on what data is being collected, why it is collected, and how it is being used. This builds public trust and allows for informed discussion about data practices.
- Robust security measures must be implemented to safeguard data from unauthorized access, breaches, or loss.
- Data collection and use should ultimately serve the public good, while balancing need for data with rights and privacy of individuals.

5.2 Data Ownership and Associated Process Parameters

5.2.1 Metadata

Metadata which refers to the data about data shall manage descriptive details such as format, source, and timestamps. These details can have privacy implications. The policy ensures that metadata is treated with confidentiality and integrity and is subject to same privacy controls as the data it describes. It also provides guidelines for the retention, access, and protection of metadata to prevent unauthorized use and to comply with legal and regulatory requirements.

5.2.2 Ownership of Data

Data Ownership is a critical component of data governance, as it ensures effective management, accountability, and utilization of data. This will be facilitated by a Data Owner or Data Delegate having following responsibilities:

- **Data Owner:** Responsible for the comprehensive management and control of specific data sets. Their duties include defining access rights, establishing usage policies, and ensuring compliance with relevant regulations.
- **Data Delegate:** In instances where the data owner is unavailable, a data delegate may assume responsibility of Data Owner to oversee the authorization process. The data delegate is tasked with ensuring that data adheres to established process flows throughout its lifecycle, maintaining data quality, verifying data accuracy, and liaising with both consumers and owners.

5.2.3 Data Classification

The process of categorizing data involves assessing its sensitivity level, value, and importance to its participating entities with respect to data sharing and consumption. SSDP classifies data into following four categories:

- **Open Access Data:** This category includes data that is openly accessible to both public and private bodies. It can be freely used and redistributed for statistical studies, economic growth, research and innovation, supply chain management, and other areas that benefit the State.
- **Registered Access Data:** This category of data is accessible only through a defined registration or authorization process. Recognized institutions, organizations, and public users can access this data through specific procedures. It primarily consists of raw data or database dumps that have been anonymized to remove identifiers, making it suitable for research purposes by academic, research, and civil society organizations.
- **Restricted Access Data:** This category includes sensitive personal data and datasets that are confidential in nature and whose disclosure could compromise the country's security. Such data falls into the negative list and is not open to the public. It includes data explicitly prohibited from sharing under Sections 8 and 9 of Right to Information Act 2005. The RTI Act 2005 and Right to Privacy Judgment of 2017 should be considered when compiling this list.

5.2.4 Consent Management

Consent Management is a critical component, as it ensures that individuals maintain control over the collection, use, and sharing of their data. Consent is also required for any revision of personal information.

The key aspects of consent management are mentioned below:

- **Explicit Consent Requirement:** Establish a mandate to obtain explicit consent from individuals before collecting, processing, or sharing their personal data. Such consent must be freely given, specific, informed, and unambiguous, demonstrating a clear affirmative action by the individual.
- **Parental or Guardian Consent:** Secure consent from parents or guardians for collection, use, updating, and processing of personal data belonging to minors (under applicable age of consent), as well as individuals who are illiterate, mentally challenged, or disabled (and unable to read/write), as determined by the State Government.
- **Consent Form:** Develop standardized consent forms or mechanisms that clearly articulate the purpose of data collection, types of data being collected, intended use of data, and who will have access to it. Options should be offered to individuals for providing or withholding consent.
- **Consent Management Platform:** A platform or tool to automate the consent process, manage consent preferences, track consent statuses, and ensure compliance with consent requirements. The platform should be user-friendly, transparent, and easily accessible.
- **Consent for Sensitive Data:** Acquire separate and explicit consent for collection and processing of sensitive personal data, such as health information, biometric data, genetic data, political opinions, religious beliefs, or other special categories of data. Emphasize the sensitivity of this data and necessity for specific consent.
- **Granular Consent Options:** Provide granular consent options that enable individuals to selectively agree to specific uses of data, sharing purposes, processing activities, and communication preferences. Offer clear choices and opt-in/opt-out mechanisms for various data processing activities.
- **Consent for Third-Party Sharing:** When sharing data with third parties, obtain explicit consent for such activities. Inform individuals about who will receive their data, purposes of sharing, and any terms and conditions associated with third-party data sharing.
- **Consent Revocation:** Empower individuals with the ability to revoke or withdraw their consent at any time, outline the process for revoking consent, including methods for withdrawing consent, updating preferences or requesting data deletion.
- **Consent Tracking and Documentation:** Keep detailed records of consent, including date and time consent was given, the extent of consent, purposes of data processing, and any conditions or limitations associated with the consent. Document any changes in consent status and requests for consent revocation.
- **Consent Audits and Compliance:** Regularly audit and assess consent practices to ensure adherence to consent requirements, data protection laws, regulations, and industry standards. Monitor consent management procedures, resolve consent-related issues, and take corrective measures as necessary.

5.2.5 Data Quality

Data quality is a crucial aspect, as it ensures that data is accurate, reliable, and fit for its intended purpose. Integrating data quality management into data governance framework outlined in SSDP is

essential. Defining roles, responsibilities, processes, and controls for managing data quality across data domains, datasets, and data lifecycle stages is necessary to maintain high data standards.

5.2.6 Data Documentation

Data documentation promotes transparency, understanding, and usability of data assets. It should involve proper data classification, appropriate metadata tagging, and access and usage parameters.

5.2.7 Data Collection

SSDP outlines processes for data collection that align with legal requirements and ethical standards by adhering to methods of transparency and consistency.

Data collection mechanism shall be integrated with government service delivery, capturing minimal information at defined intervals to make the overall data collection method transparent. SSDP defines a consent-based process to make the data collection approach robust and compliant. The preferred data collection modality should be electronic to facilitate verification and automated processing.

5.2.8 Data Storage

The storage of Data is a critical aspect of SSDP. It involves safeguarding state data with the CIA (Confidentiality, Integrity, and Availability) triad model. Data storage must be safeguarded through encryption, strict access controls, regular backups, and compliance with relevant security regulations to ensure its confidentiality, integrity, and availability.

The data custodian is responsible for managing and safeguarding data assets, ensuring compliance with security protocols, maintaining data integrity, and facilitating secure access and storage practices.

Establishing a data retention policy is crucial to specify how long data will be retained based on legal requirements, business needs, and data usage purposes. It is important to define criteria for data retention, archival, and disposal to manage the data lifecycle effectively.

In alignment with the Digital Personal Data Protection (DPDP) Act 2023, any data stored in cloud environment must comply with defined security and privacy norms. This includes clear identification of data storage locations, prioritizing localization within India, ensuring encryption for data at rest and in transit, enforcing role-based access, and maintaining audit logs for traceability. Cloud service providers must support timely breach notification, enable secure deletion and portability of personal data, and align with state-approved retention and disposal standards to uphold the rights of data principals and integrity of the state's digital ecosystem.

5.2.9 Data Interoperability

Data Interoperability in SSDP enables different systems and organizations to share and utilize data seamlessly. It involves standardizing data formats and protocols to ensure consistency and compatibility across various platforms. An effective data governance framework oversees data sharing, ensuring quality and privacy.

5.2.10 Data Access Protocol and Authentication

Data access and authentication specifies who can access data and outlines the process for obtaining such authorization. It is largely dependent on the individual's role within the organization, with access rights being granted based on the necessity to know for job functions. The principle of least privilege is enforced to provide only the minimum level of access needed for task completion.

A formalized process must be in place for requesting access, which involves supervisor approval and a review by the IT or Data Security team. Authorization is given by data owners or managers after verifying that the access aligns with individual's responsibilities. Verification methods are to be identified such as multi-factor authentication, to prevent unauthorized access.

Regular reviews of data access ensure that rights remain appropriate, with access being revoked when it is no longer needed or upon role changes. An audit trail is maintained for all authorizations to ensure accountability and oversight, thus maintaining the security and integrity of data.

5.2.11 Data Sharing

SSDP facilitates collaboration, improves services, and supports data-driven decision-making while safeguarding privacy and security. It implements a data governance framework that includes policies, procedures, and oversight mechanisms for managing data-sharing activities. Defining roles and responsibilities for various process owners is essential to ensure accountability and transparency in data-sharing practices. Establishing formal data-sharing agreements or contracts between parties involved in data sharing is also important.

Geo-spatial data sharing plays an important role in planning, governance, and service delivery. By sharing location-based data such as maps, land records, and infrastructure details among departments, duplication of efforts can be avoided, and decision-making becomes faster and more accurate. It also helps improve coordination between departments and supports public services like disaster management, agriculture, and urban planning. The data should be shared in standard formats with proper documentation, while ensuring privacy and access control for sensitive information. Encouraging open and secure geo-spatial data sharing can also support innovation, research, and the development of digital tools and applications.

5.2.12 Data Security

Data Security is a critical component of SSDP, designed to protect sensitive information, prevent unauthorized access, and safeguard data integrity. This is achieved by implementing data encryption methodologies, data loss prevention strategies, and access controls. It is important to develop and implement an incident response plan to effectively respond to data security incidents, breaches, or cyberattacks. This plan should define roles and responsibilities, incident detection and reporting procedures, containment measures, forensic analysis, and communication protocols. Additionally, providing security awareness training and education to employees, contractors, and stakeholders is

essential to promote good cybersecurity practices, threat awareness, data protection principles, and incident response procedures.

5.2.13 Data Privacy

Data privacy refers to specific rules and guidelines that govern the collection, storage, use, and sharing of personal information within a department/organization. SSDP is designed to protect individuals' personal data from misuse and ensure compliance with relevant data protection laws and regulations.

5.2.14 Data Retention and Archival

Data retention is an important aspect of data policy which refers to the process of storing and maintaining data for a specified period to meet the legal, regulatory, operational, or business requirements. It will ensure that data is preserved for as long as necessary for specific purposes and disposed of or deleted once it is no longer required.

The retention and archival periods of data will be defined by the data steward who ensures data quality, integrity and proper management of departmental data by overseeing all stages of data lifecycle in alignment with established data governance principles and existing retention policy of government. Priority should be given to data whose utility is time sensitive and such data shall be surely retained.

Data archive in Sikkim State Data Policy (SSDP) refers to a centralized repository where government data is systematically stored, managed, and made accessible for analysis and public use, ensuring transparency, accountability, and informed decision-making. It often includes guidelines for data preservation, security, and usage to support research and policy development.

5.2.15 Data Destroy

Data Destruction is a critical component of a comprehensive data policy, ensuring that data no longer required is permanently deleted in a secure and compliant manner. This step prevents unauthorized access to sensitive information and mitigates risks associated with data breaches or misuse. A well-defined data destruction policy outlines the procedures, timing, and methods for securely erasing data from all storage systems. Implementing a structured data destruction policy helps organizations maintain compliance, reduce storage costs, and mitigate potential legal and security risks.

5.2.16 Data Currency

Data Currency refers to the real-time value and relevance of data, crucial for businesses that rely on up-to-date information for accurate insights and decision-making. It involves real-time data updates, synchronization across databases, and classification based on relevance, ensuring that organizations work with the freshest data available. While offering benefits like improved customer targeting, risk management, and enhanced business performance, maintaining data currency also presents challenges, including resource consumption and managing data consistency. In a Data Lakehouse environment, where structured and unstructured data coexist, maintaining high data currency is vital

for precise analytics. Security measures like encryption and access control are essential during data updates.

5.2.17 Cross Border Data Transfer

Cross-border data transfer refers to the movement or transfer of any type of data, including personal and sensitive personal data of individuals, or data from non-government entities associated with Sikkim State Government within the jurisdiction of Sikkim to locations outside India. This transfer may occur for purposes such as processing, storage, analysis, or other activities by government or non-government entities, or service providers located outside India.

As per the section 14 of DPDP Rules 2025, the following considerations are to be adhered to for cross border transfer of personal data:

Transfer of personal data processed by a Data Fiduciary -

(a) within the territory of India; or

(b) outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India, is subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.

To ensure compliance with the above, following key factors must be considered:

Compliance with National Laws: Any transfer of personal data outside India must comply with DPDP Act 2023 or any other applicable national legislation related to data protection and privacy. However, as per data localization requirements, certain types of data, such as sensitive personal data and critical personal data, may need to be stored and processed within India or subject to specific conditions and safeguards before being transferred outside India.

Government-Approved Countries: Data can only be transferred to countries or regions that the Indian government deems to have adequate data protection standards. Data must only be transferred to those countries that have data protection laws and practices in place to ensure secure and privacy-compliant processing and storage.

Data Protection and Security: Departments must implement stringent data security measures and data protection standards to ensure privacy and integrity of the transferred data, in compliance with both national and international data protection norms.

5.3 Platform

5.3.1 Sikkim Data Bank

The Sikkim Data Bank will be a centralized platform or website that provides access to various datasets, information, and resources managed by state government and its agencies. It shall have the following functionalities:

- **Data Catalog:** The state data portal should include a comprehensive data catalog that lists available datasets from different government department and participating agencies. Each dataset entry in the catalog should provide metadata such as data description, source agency, update frequency, data format, and download options.
- **Data Search and Discovery:** Robust search and discovery functionalities within the data portal to allow users to easily search for specific datasets, keywords, topics, or categories. Filters, tags, and advanced search options may be provided to refine search results.
- **Data Visualization Tools:** Data visualization tools and interactive dashboards to visualize and analyze data from the data portal.
- **API Access:** Provide application programming interfaces (APIs) that allow developers, researchers, and businesses to access and integrate datasets from the data portal into their applications, websites, and services. Offer documentation, API keys, and developer resources for API usage.
- **Data Download Options:** Enable users to download datasets from the data portal in multiple formats such as CSV, Excel, JSON, XML, or geospatial formats. Provide bulk download options, data subsets, and data export functionalities for different user needs.
- **Data Quality Information:** Include data quality information, documentation, and metadata standards for datasets available on the data portal. Provide data quality scores, data validation reports, and data lineage information to help users access data reliability and accuracy.
- **Data Licensing and Usage Terms:** Specify data licensing terms, usage restrictions, and terms of use for datasets available on the data portal. Provide information about data reuse, attribution requirements, commercial use, and any restrictions or limitations associated with data usage.
- **User Feedback and Collaboration:** Allow users to provide feedback, comments, and ratings for datasets on the data portal. Encourage user collaboration, data sharing, and community engagement through forums, discussions, and collaboration platforms.
- **Data Transparency and Open Data Initiatives:** Promote data transparency and open data initiatives by publishing Government data, reports, and information on the data portal. Support open data principles, data sharing practices, and data-driven decision-making across Government agencies and stakeholders.

5.3.2 IT Systems and Solutions

SSDP, IT systems and solutions shall play a crucial role in enabling data management, privacy protection, security, and compliance. The various IT systems are mentioned below:

- **Data Management Systems:** Robust data management systems such as data warehouses, data lakes, and Master Data Management (MDM) solutions to centralize, integrate, and manage data from multiple sources. Ensure data governance, data quality, and data lifecycle management capabilities within data management systems.
- **Data Integration Platforms:** Deploy data integration platforms and ETL (Extract, Transform, Load) tools to facilitate seamless data integration, data migration, and data synchronization across disparate IT systems and data sources.
- **Cloud Computing Services:** Leverage cloud computing services like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) for scalable and flexible IT infrastructure. Use cloud storage, cloud databases, and cloud analytics services for data storage, processing, and analysis.
- **Cybersecurity Solutions:** Implement cybersecurity solutions like firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint security, encryption tools, and security information and event management (SIEM) systems to protect IT systems and data assets from cyber threats and attacks.
- **Data Encryption and Privacy Enhancements:** Use data encryption tools, encryption algorithms, and data masking techniques to encrypt sensitive data at rest and in transit. Implement privacy-enhancing technologies (PETs) such as differential privacy, homomorphic encryption, and anonymization for data privacy protection.
- **Disaster Recovery and Service Continuity:** Implement disaster recovery (DR) solutions, backup and restore mechanisms, and business continuity plans to ensure IT system resilience, data recovery, and continuity of operations in case of IT disruptions, data loss, or disasters.
- **Emerging Technologies Integration:** Explore emerging technologies such as Blockchain, Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), and edge computing for potential integration into IT systems. Assess benefits, risks, and use cases of emerging technologies in data management and governance.
- **Data Analytics and BI:** Utilize data analytics and BI tools (data analytics platforms, dashboard tools, reporting tools, and predictive analytics capabilities for data-driven decision-making) to analyze, visualize, and derive insights from data stored in IT systems.

6 Implementation Framework

SSDP will be put into action through a systematic approach that turns policy goals into practical steps, procedures, and programs.

Department of Information Technology, Govt. of Sikkim, will act as a central agency overseeing the policy's rollout. The policy will apply to all state departments, public sector undertakings (PSUs), and state-level Government bodies to ensure comprehensive data collection and widespread benefits throughout the state.

Effective implementation will require collaborative efforts and robust governance. Engaging key stakeholders, such as Government departments, PSUs, agencies, data owners, data privacy officers, and legal advisors, is essential for a successful implementation process.

6.1 Governance Committees, Framework, Roles and Responsibilities

The Governance Committees will be responsible for overseeing implementation of the policy. These Committees will establish clear guidelines for data collection, management, sharing, and security. It emphasizes compliance with national and state-level data protection regulations, ensuring that all Government departments adhere to these standards. The framework encourages interdepartmental coordination, fostering efficient data exchange while reducing redundancy.

Additionally, it incorporates training and capacity-building programs to enhance skills of Government employees in data-related roles. This structured approach ensures transparency, promotes data-driven decision-making, and encourages citizen engagement through public data platforms and consultation processes.

6.1.1 State Data Steering Committee (SDSC)

The State Data Steering Committee (SDSC) will be a key authority responsible for overseeing the data policy of Sikkim. Proposed to be chaired by Chief Secretary to Government of Sikkim, with Secretary to Government (IT Department) as Convener-cum-Member Secretary, the committee comprises of senior Government officials are along with representatives from academia.

6.1.1.1 Administrative Framework

- **Chairperson**: Chief Secretary to Government of Sikkim.
- **Convener-cum-Member Secretary:** Secretary to Government (IT Department)

❖ **Members:**

- Principal Secretary, Women & Child Development Department
- Principal Secretary, Tourism & Civil Aviation Department
- Principal Secretary, Rural Development Department (RDD)
- Controller-Accounts-cum-Secretary, Government (Finance Department)
- Secretary, Education Department
- Secretary, Land Revenue and Disaster Management Department
- Secretary cum PCCF Forest & Environment Department
- Secretary, Social Welfare Department
- Secretary, Health & Family Welfare Department
- Secretary, Agriculture Development Department
- Director General Directorate, Economic Statistics & Monitoring and Evaluation (DESME)
- Director General of Police, Sikkim Police

In addition to above proposed members, SDSC may appoint individuals with experience and qualification in fields related to IT, GIS and other relevant areas as decided.

6.1.1.2 Roles & Responsibilities

The key activities to be carried out by SDSC are as follows:

❖ Guiding departments on the use of data and information in the state's developmental planning processes.

❖ Promote and facilitate sharing of data and information among state Government departments and other users, with a focus on policy formulation and implementation for development and sustainable use of geospatial databases.

❖ Review and monitor the implementation of data sharing and accessibility plans across various Government departments.

❖ Utilize the ecosystem of service providers and leverage technical capabilities of users with mobile and social connections to enhance data accessibility and utilization.

❖ Spread awareness within community, including developers, researchers, startups, and industries, about the importance and potential applications of data-driven approaches.

6.1.2 State Data Governance and Technical Advisory Committee (SDGTAC)

The State Data Governance and Technical Advisory Committee (SDGTAC) plays a crucial role in overseeing and guiding the data governance framework within the state of Sikkim. The committee is responsible for establishing policies and standards for data management, ensuring data security, and promoting the efficient use of data to improve government services. The Chairperson, who is the Secretary to the Government of Sikkim's Department of Information Technology, leads the committee with the support of the Convener-cum-Member Director, the Director of Information Technology. The SDGTAC's members, including senior officials from various state government departments such as

Finance, Planning & Development, Law, and Rural Development, bring a wealth of expertise to the table. The Chief Data Officer, appointed by the State Data Steering Committee (SDSC), plays a pivotal role in implementing data governance strategies and ensuring compliance with data-related policies.

6.1.2.1 Chief Data Officer (CDO)

The Chief Data Officer shall be appointed by State data Steering Committee SDSC, and shall be responsible for day-to-day implementation of the State Data Policy, as well as for data management and governance, and effective utilization of data across the government:

- Lead all the data initiatives of the Government of Sikkim; and own the critical data quality and data sharing efforts such as developing Meta-Data Catalogue and Standards.
- Lead on cross-department analytics initiatives for enhanced performance by departments and improved delivery of public service and benefits to citizens; and help departments in minimizing inclusion and exclusion errors in schemes.
- Chair the DIDC which is responsible for taking decisions on all aspects of data-governance, and to help collect, collate, process and publish data in line with SSDP.
- Define appropriate process for the identifying and releasing open access datasets. Proactively release as many datasets as possible under Open Access Data classification.
- Ensure data privacy of the Data Principals and citizens while sharing data with all appropriate and possible safeguards
- Recommend to the Chairperson of CDM for approval on the department specific Negative List of confidential datasets prepared by DIDC in consultation with respective departments/institutions/autonomous bodies.
- Work with the Data Principals and Processors to help transform departmental data into actionable insights for targeted policy interventions or even identifying gaps in service / benefit delivery.

6.1.2.2 Administrative Framework

- **Chairperson**: Secretary to Government of Sikkim, Dept. of Information Technology (IT)
- **Convener-cum-Member Director**: Director of Information Technology (IT Department)
- **Members**: Nodal officers selected by concern Department from following state Government departments:
    - Chief Data Officer (to be appointed by SDSC)
    - Finance
    - Planning & Development
    - Law
    - Rural Development Department (RDD)
    - Directorate of Economic Statistics & Monitoring and Evaluation (DESME)

6.1.2.3 Roles and Responsibilities

SDGTAC will oversee and manage all aspects of data governance within the state, ensuring that data is handled securely, ethically and effectively. This committee combines governance oversight with technical expertise to promote data-driven decision-making across Government departments. The key activities to be carried out by SDSC are as follows:

- Supervise management of data within the state, ensuring that data is handled properly, securely, and ethically, while adhering to regulatory requirements, to safeguard privacy and confidentiality.
- Develop policies and guidelines for collection, storage, sharing, and utilization of data across various Government departments, promoting consistency and compliance.
- Oversee the technical aspects of data management, including data structure, source validation, data storage processes, security, and incorporation of emerging tools and infrastructure.
- Provide leadership support in implementing data-related projects, ensuring they align with the proposed technical framework.
- Foster collaboration among different departments to facilitate efficient data sharing and utilization, reducing duplication and promoting synergy across state government departments.
- Encourage adoption of new technologies for data management and analysis, ensuring that the state remains at forefront of data-driven governance.
- Support capacity building initiatives aimed at enhancing data literacy and technical competency of government employees, enabling them to use data effectively and responsibly in their roles.

6.1.3 Department Level Committee

The Department Level Committees will be established to oversee implementation, management, and compliance of department's data governance framework. The committee ensures that all data-related activities within department align with the state's overall data policy, enabling efficient data management, quality assurance, and secure data sharing.

6.1.3.1 Administrative Framework

- **Chairperson:** Department Secretary
- **Members:**
  - Department Data Officer
  - Department Sub Data Officer
  - Data Coordinator
  - Data Advisor

6.1.3.2 Roles and Responsibilities

The Department Level Committee shall be responsible for leading the review and implementation of SSDP within the department. It will ensure alignment with departmental objectives, approve recommendations, and oversee the assessment of current data practices. The committee will identify gaps, provide feedback on policy's impact, and support the Data Officer in compiling necessary data.

Additionally, it will implement department-specific initiatives in line with policy guidelines to enhance data management. The key activities to be carried by Department Level Committee are as follows:

- Lead the policy review process at department level.
- Ensure that all activities align with departmental objectives.
- Approve department-specific recommendations for policy implementation.
- Oversee assessment of current data practices within the department.
- Identify gaps and areas for improvement in data management.
- Provide detailed feedback on the policy's impact on departmental data management.
- Assist in the review and analysis of departmental data management practices.
- Support the Data Officer in compiling relevant data and information for policy review.
- Implement department-specific data initiatives according to the policy guidelines

7 Legal Framework

The data policy's legal framework is shaped by a range of Indian laws, rules, and regulations focused on data protection, security, and privacy. It also considers any existing or forthcoming state-specific data regulations. The objective of these laws and policies is to safeguard individual privacy, secure data, and encourage ethical and efficient use of data. Departments and Government entities may each have specific protocols for managing data. These protocols dictate the methods for data collection, storage, processing, access, sharing, and eventual disposal. Data gathered by each department is considered its property and may be shared via their IT systems and applications to facilitate access and collaboration.

To establish a robust legal framework, all departments within the State Government should adhere to the following acts, policies, rules, and regulations. These provisions are instrumental in addressing various cases and scenarios, ensuring smooth and effective data governance.

- Information Technology (IT) Act, 2000: *Governs electronic commerce, cybercrime, digital signatures, along with other aspects of IT.*
- Aadhaar Act, 2016: *Regulates use of Aadhaar numbers for identity verification and related services.*
- Digital Personal Data Protection (DPDP) Act 2023: *Establishes a framework for the protection of personal data and privacy.*
- National Data Sharing and Accessibility Policy, 2012: *Promotes open access and sharing of government data for public use.*
- Right to Information Act, 2005: *Provides citizens right to access information from public authorities.*
- Telecom Regulatory Authority of India (TRAI) Regulations: *Regulates the telecom sector to ensure fair practices and consumer protection.*
- Bhartiya Nyaya Sanhita (BNS), 2023: *Reforming the criminal justice system, emphasizing victim rights and expediting legal processes.*
- Indian Contract Act, 1872: *Governs the formation and enforcement of contracts in India.*
- National Digital Communications Policy (NDCP), 2018: *Aims to provide universal broadband access and boost the digital economy.*
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: *Specifies security practices for handling sensitive personal data.*
- Draft Data Empowerment and Protection Architecture (DEPA): *Proposes a framework to empower individuals with control over their personal data.*

8
Data Monetization

Sikkim State Data Policy encourages the use of non-sensitive data and supports sustainable practices by monetization, prioritizes equity, privacy, and open data principles.

The policy outlines that there will be fees for accessing data, but educational, nonprofit, and low-income users may qualify for waivers. Different payment methods will be available, ensuring transparency and fairness in pricing.

Charges for data access may vary based on how much data is used (volume-based) or how much demand is there (usage-based). Custom requests for data and licensing fees will depend on factors such as how the data is gathered, how complex it is, and what it will be used for.

The cost should be determined based on the following criteria:

- **Data Type:** Different types of data should be priced based on how sensitive and important they are.
- **Data Volume:** Larger sets of data generally cost more because of their volume.
- **Data Recency:** Newer data is usually more valuable, so its price should reflect accordingly.
- **Data Usage Rights:** The price of data depends on how buyer can use it, like one-time use, long-term use, exclusive rights.
- **Market Demand:** Data that is in high demand in the market will be more expensive.

9 Conclusion: Policy Review, Update, Training and Awareness

9.1 Review Process

As part of review process, the Chief Data Officer (CDO) will review policy adherence and compliance twice a year. Additionally, at the end of each year, an independent check called Data Protection Impact Verification (DPIV) will be done to identify and fix any risks related to personal data collection and processing. The findings of these reviews will be sent to SDSC for further review and recommendations. The SDSC will then prepare an annual report on how well the policy is being followed and submit it to the Cabinet for evaluation.

Furthermore, an independent third-party evaluation will be carried out annually to assess how well the policy is being put into action. This evaluation will focus on data handling and usage alignment with the policy and also understanding of challenges in application of the policy, as well as ongoing mitigation efforts. The CDO, supported by SDSC and Department Data Officers supervised by their respective Administrative Secretaries will work with third parties to conduct such evaluation.

9.2 Update Process and Frequency

The SDSC, in consultation with SDGTAC, will update this policy once in every two years. These updates will ensure the policy stays current with new laws, infrastructure, and other developments.

9.3 Training and Awareness

The goal of training programs is to make sure that employees of Government of Sikkim have the necessary skills and knowledge to handle data effectively. This will help them make informed decisions based on data at every level.

SDSC, along with relevant departments and a team of training experts, will create a detailed plan to train and improve the skills of Government employees who work with data. Each department will develop online training curriculum that officials and staff can access to enhance their data-related skills.

The responsible department will oversee creation, maintenance, and regularly updating of content related to data governance. This includes how data is handled, managed, and used. The same department will also manage information about the IT infrastructure and procedures used for data collection,

processing, management, and use. They will set up a unified platform where all Government officials and staff can access and use these training materials.

The Chief Data Officer, guided by SDSC, will manage the coordination and execution of training and capacity development programs. This will involve working closely with Department Data Officers. The training will be tailored to meet specific needs of different roles within the data governance and management framework, with a special emphasis on improving skills of district-level officers and staff who handle data collection, cleaning, management, reporting, and processing.

Departments are encouraged to collaborate with universities, academic institutions, and experts to create and deliver capacity building programs, promote data-driven innovations, and launch related projects. These efforts will be reviewed and recognized by SDSC.

10
Budget Provisioning

The implementation of SSDP shall involve costs for both data custodians and data administrators, covering aspects such as data conversion, refinement, storage, and quality enhancement. Relevant departments and public organizations may request necessary budget allocations from the Department of Finance to support these expenditures. Furthermore, the Government of Sikkim will need to invest a significant amount of budget, through IT and cloud infrastructure at SDC, to meet increased demands for data storage and network computing capabilities from various Government departments.

Each department will have a specific budget section dedicated to improving their data systems. This budget will be allocated exclusively for software systems and resources involved in strengthening data systems. No funds from this budget will be spent on purchasing and installing server hardware, as this often leads to unnecessary duplication of public resources.

Annexure

A. Feedback Loop for SSDP

Feedback mechanisms will be established and communicated through various channels, allowing public and relevant stakeholders from State Government departments suggest improvements to the draft policy document.

Below is a sample form for the Feedback Loop, which may be made accessible via relevant link on IT Department web portal at https://www.sikkim.gov.in/departments/information-technology-department, to allow sharing of suggestions on SSDP. Such feedback will be invaluable in refining and enhancing the policy, by incorporating constructive suggestions.

Feedback on Sikkim State Data Policy 2025

Feedback by:	☐	Public	☐	State Department
			Select Department: *(Enable when State Department chosen)*	Choose an item
INFORMATION ON FEEDBACK PROVIDER				
Full Name:			Designation: *(Enable when 'Feedback by' chosen as State Department)*	
Email Id:				
Phone No:				
Feedback Title:				
Draft Policy Section Name:			Choose an item *(Section of the Policy to be selected from the Dropdown)*	
Feedback Details:				
Captcha: UR9N6				

Submit

***Note:** Please note that the sample screenshot of the feedback form displayed above is a preliminary design and will be updated with precise graphic representation once the form has been reviewed and finalized. 'Annexure A' will be removed from the policy once it is approved. The finalized form will be available on the designated web portal for public and departmental feedback.*

B. Bi-Lingual version of SSDP

SSDP may be considered to be drafted in a bilingual format, both in Nepali and English. A bilingual policy document would demonstrate Sikkim's dedication to foster its regional language, while also ensuring clear and accessible communication for residents who speak only Nepali. Additionally, those proficient in Nepali will be able to directly access and comprehend the policy without facing any language obstacles.