KPMG Advisory Services Private Limited
Unit No. A505,
5th Floor, Elante Offices,
Plot No.178-178A, Industrial Area, Phase -1,
Chandigarh-160002

Telephone: +91 172 664 4000
Fax : +91 172 664 4004
Internet: www.kpmg.com/in
Email:indiawebsite@kpmg.com

Strictly Private and Confidential

Mr. Ambrish Shahi
Sr Social Protection Specialist
The World Bank Group
70 Lodi Estate
New Delhi 110 003
India

13 June 2022

Subject: Draft Punjab State Data Policy: Operational Guidelines

Dear Ambrish,

We appreciate the opportunity to assist The World Bank Group in Analysis, Research, Sharing Best Practices and Recommendations on State Data Policy in Punjab State.

Please find enclosed our draft-report, which has been prepared in accordance with the scope and terms stated in our contract No 7201090 dated June 01, 2021, for your perusal. Please let us know your feedback.

It has been our privilege to have this opportunity to work with you, and we look forward to continuing our relationship.

Yours sincerely

Himanshu Rattan
Authorised Signatory

Disclaimer and Notice to Reader

1. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.
2. We have prepared this report solely for the purpose of providing select information on a confidential basis to the management of The World Bank Group in accordance with the contract No 7201090 dated June 01, 2021executed between The World Bank Group and us ("Contract").
3. This report is confidential and for the use of management only. It is not to be distributed beyond the management nor is to be copied, circulated, referred to or quoted in correspondence, or discussed with any other party, in whole or in part, without our prior written consent, as per terms of business agreed under the Contract.
4. This report sets forth our views based on the completeness and accuracy of the facts stated to KPMG and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions.
5. While performing the work, we assumed the genuineness of all signatures and the authenticity of all original documents. We have not independently verified the correctness or authenticity of the same.
6. We have not performed an audit and do not express an opinion or any other form of assurance. Further, comments in our report are not intended, nor should they be interpreted to be legal advice or opinion.
7. While information obtained from the public domain or external sources has not been verified for authenticity, accuracy or completeness, we have obtained information, as far as possible, from sources generally considered to be reliable. We assume no responsibility for such information.
8. Our views are not binding on any person, entity, authority or Court, and hence, no assurance is given that a position contrary to the opinions expressed herein will not be asserted by any person, entity, authority and/or sustained by an appellate authority or a court of law.
9. Performance of our work was based on information and explanations given to us by the Officers & Officials of the Government of Punjab. Neither KPMG nor any of its partners, directors or employees undertake responsibility in any way whatsoever to any person in respect of errors in this report, arising from incorrect information provided.
10. Our report may make reference to 'KPMG Analysis'; this indicates only that we have (where specified) undertaken certain analytical activities on the underlying data to arrive at the information presented; we do not accept responsibility for the veracity of the underlying data.
11. If any extracts of such editable version of the Report are shared with third parties, it should be done without any reference to our name and logo in any manner whatsoever.
12. In connection with our report or any part thereof, KPMG does not owe duty of care (whether in contract or in tort or under statute or otherwise) to any person or party to whom the report is circulated to and KPMG shall not be liable to any party who uses or relies on this report. KPMG thus disclaims all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such third party arising out of or in connection with the report or any part thereof.
13. By reading our report the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.

Draft Punjab State Data Policy: Operational Guidelines – Part 1

Draft Guidelines and Implementation Manual for the Department of Governance Reforms and Public Grievances

March 2022

Contents

Sl. No.	Document Name	Version History	Created By	Reviewed By	Approved By	Submitted On
1.	Punjab State Data Policy: Operational Guidelines	01	KPMG	World Bank	N/A	16 November 2021
2.	Punjab State Data Policy: Operational Guidelines (Part 1, 2 & Annexure)	02	KPMG	DGRPG	N/A	02 March 2022
3.	Punjab State Data Policy: Operational Guidelines (Part 1, 2 & Annexure A, B, C, D, E)	03	KPMG	Government of Punjab, J-PAL, Artha	N/A	23 March 2022
4.	Punjab State Data Policy: Operational Guidelines (Part 1, 2 & Annexure A, B, C, D, E)	04	KPMG	TBA	TBA	13 June 2022

1 Introduction to the Operational Guidelines

1.1 Overview

The Punjab government envisions a digitally empowered state and has formulated a comprehensive Data Policy in the form of the Punjab State Data Policy (PSDP). The PSDP aims to serve as a guiding instrument to promote inclusive development in the state of Punjab. The data policies formulated in PSDP aim to nurture a data-driven culture in the state of Punjab and would lay down a blueprint for a digitally empowered Punjab resulting in improved governance and citizen satisfaction.

PSDP is part of Punjab government's vision to achieve socio-economic development and inclusive growth by optimal utilization of data and technology. Through this policy, the state aims to nurture a data-driven governance ecosystem. Through PSDP, the government reiterates its firm belief that optimal governance decisions can be taken by leveraging the power of data and technology while ensuring citizen privacy and security.

In this context, a streamlined Operational Guideline is being laid down for the supervision and enforcement of the PSDP.

Formulation of these Guidelines is imperative as it sets uniform standards and procedures for the Department of Governance Reforms and Public Grievances (DGRPG), all state departments, defines rules on collection, processing and management of data while giving utmost importance to laws, citizen privacy, security, and rights.

These guidelines will serve as an institutionalized framework for data management and would define clear rules of engagement across all the state departments with respect to data management.

1.2 Objective of the Operational Guidelines

The primary motive of the guidelines is to lay down policies and standards for legal and ethical management of data holdings of the Government of Punjab and to ensure safe data practices. It would also define the principles to identify the people responsible for its enforcement and aims to define clear delegation of authority and responsibilities.

The guidelines will help to extract value from all the data already being held by the state and to be collected in future, and will aim to enable greater data access, shareability and integration at the state level and would play a vital role in increasing overall efficiency and accountability.

1.3 Scope of the Operational Guidelines

This framework applies to all data and information created, generated, collected, and processed using public funds provided by the Government of Punjab, Central Government funds, and international donor organizations, directly or through authorized agencies by various Departments/ Organizations/Agencies and Autonomous bodies.

1.4 Applicability of the Guidelines

The overall framework must be adopted by all Departments of the Government of Punjab to be fully compliant to the Punjab State Data Policy.

1.4.1 Applicability of Part 1 of the Guidelines

Part 1 of the Guidelines outline the framework and the implementation of the PSDP through the DGRPG.

1.5 Access for Data

All personal data held by the government will be governed by collection modalities and access restrictions mentioned in these guidelines, which are in consonance with the PSDP, the Information Technology Act (Privacy Rules) 2011, Information Technology Act 2000 and the Draft Personal Data Protection Bill 2019. All the Open Access Data sets will be available on Punjab Government's branch of the National Open Government Data (OGD) Platform: https://punjab.data.gov.in

2 Establishment of Apex Implementation Authorities

2.1 Punjab State Data Steering Committee

The DGRPG is the nodal department for defining, maintaining, and tracking the benchmarks on data security and protection for Open Access, Personal/sensitive personal and registered access data within the Government of Punjab. As mandated by the PSDP, the DGRPG will create the State Data Steering Committee (SDSC), to act as the apex decision making body within the DGRPG. The *SDSC will be chaired by the Chief Secretary to the Government of Punjab* and comprise of the following members:

- Administrative Secretary, DGRPG
- Administrative Secretary, Department of Planning
- Director, Governance Reforms, DGRPG
- Chief Data Officer, Government of Punjab (Refer to Section 2.2)
- 3-5 officers/experts, as nominated by the Chief Data Officer (Refer to Section 3.2)
- Departmental Data Officers for each Department under the Government of Punjab (Refer to Operational Guidelines – Part 2, Section 2.1.2)
    - Departmental Data Officers will be present only in an advisory capacity and the final decision-making authority will solely rest on the Chairperson and remaining members of the SDSC

The composition of the Committee may be reviewed and revised as and when needed and at least once in every 6 months. The Director, DGRPG shall act as the Convener for this Committee.

2.1.1 Roles and Responsibilities

The SDSC will be the nodal body within the DGRPG which will decide on the course of action for any data related initiative of the Government of Punjab. The SDSC will have the following responsibilities:

- Nominate the Chief Data Officer
- Oversee the establishment, functioning and periodic review of the PSDP Project Management Unit (PMU) (Refer to Section 3)
- Oversee the establishment of Departmental Data Cells (Refer to Operational Guidelines – Part 2, Section 2.1)
- Oversee the establishment of the District Data Cells (Refer to Section 4)
- Oversee the development and implementation of a Data Exchange Platform and subsequent Open API e-Governance System based on principles outlined in these guidelines (Refer to Section 8)
- Oversee Departmental Compliance to the PSDP and its guidelines
- Adjudicate on any Breach of Personal/Sensitive Personal Data held by the Government of Punjab, in case of escalation (Refer to Operational Guidelines – Part 2, Section 4.2.4.2)
- Oversee the establishment of the Expert Group for Data Governance in Punjab (Refer to Section 2.3)
- Nominate Members of the Expert Group on Data Governance (Refer to Section 2.3.2)

- Lay down the allocation of tasks between the Chief Data Officer and other relevant authorities of the PMU
- Notify further tasks for itself as it may see fit during periodic reviews

2.2 Chief Data Officer, Government of Punjab

2.2.1 Nomination

The SDSC will nominate the Chief Data Officer (CDO) for the State of Punjab which will then be ratified by the Governor of the State. The CDO at the date of his/her respective appointment must have the following qualifications:

- Have held Public Office for at least ten years either under the Government of India or in the Government of Punjab
- Recent Public Office held must be related to Information Technology or Governance Reforms (e.g., Director, DGRPG or Director, Department of Information Technology)

The CDO will hold office for a maximum term of six years from the date on which he/she enters upon his/her office or until he/she attains, the age of sixty-five years. All other regulations under the Punjab Civil Services Code relating to Personnel Appointment will be applicable for this appointment.

2.2.2 Roles and Responsibilities

The CDO will be responsible for enforcing the PSDP and its guidelines throughout the Government of Punjab along with offering advice and assistance to the SDSC and the individuals or groups whose information is being held. The CDO will also act as the adjudicating authority in case of any breach of the PSDP and its guidelines, as a part of the SDSC and advise on necessary remedial actions.

The responsibilities of the CDO are as follows:

- Head the PSDP Project Management Unit (PMU)
- Convene the meetings of the PSDP PMU and prepare its agenda
- Ensure the timely performance of the tasks of the SDSC and the PSDP PMU
- Act as the grievance redressal officer for citizens in case an issue is escalated to the level of the SDSC (Refer to Operational Guidelines – Part 2, Section 4.2.4.2, for initial grievance redressal)

2.3 Expert Group for Data Governance

The PSDP calls for the establishment of an Expert Group on Data Governance to address the challenges posed by the use of data for the delivery of state services. This Expert Group will be an impartial advisory body which will provide expertise to the SDSC for the development of further strategies and guidelines on the use of data and AI, while preserving their transformative value for the achievement of the Agenda of the PSDP.

The Group will consist national/international leaders from the public sector, civil society, private sector, and legal community who are not currently affiliated with the Government of Punjab. Group members will serve in their personal capacity, not as representatives of their affiliated organizations. Opinions and feedback will be based on members' own field of expertise and informed by privacy principles and ethical standards outlined in these guidelines.

2.3.1 Roles and Responsibilities

The Expert Group will dispense the following functions:

- Advise the SDSC on matters of Data Usage and Privacy as put forward by the PSDP PMU
- Advise the SDSC on usage and adoption of new technologies
- Advise the SDSC on cases regarding the breach of the Open Data License and Personal/Sensitive Personal Data (Refer to Operational Guidelines, Part 2 – Section 4.1.1.4 & Section 4.2.4.2)
- Advise the SDSC on decisions regarding the ethical usage of Data, as put forward by the Ethics Committee (Refer to Section 5)
- Advise on complying with guidelines and protocols for data sharing

2.3.2 Nomination of Members

Due to the Expert Group being an independent impartial body, the appointment of its members will be at the *discretion of the SDSC and the Chief Secretary, Government of Punjab*. However, the following parameters are to be considered during such appointment:

- Members must be leaders in the respective fields
- Members must be in a field related to Computer Science, IT, Data Analytics, Policy, Law, Industry, Economics, Statistics, and other associated fields
- Members must have a proven track record on delivering high-impact solutions to problems in their respective fields
- Members must not be affiliated to any Political outfit and must not have any prior criminal record

2.3.3 Compliance Grid for Establishment of Apex Implementation Authorities

Steps to be taken	Creator	Checker	Approver
Establishment:			
Step 1: Establish Punjab State Data Steering Committee with proposed members	DGRPG	Chief Secretary, Government of Punjab	Governor of Punjab
Functions:			
Step 1: State Data Steering Committee to nominate Chief Data Officer, Government of Punjab	Members of the SDSC	Chief Secretary, GoP	Chief Secretary, GoP
Step 2: Chief Data Officer to nominate 3-5 support staff (Subject Matter Experts) to act as the PSDP Project Management Unit (PMU)	CDO	Members of the SDSC	Chief Secretary, GoP

Step 3: State Data Steering Committee to nominate Expert Group for Data Governance in Punjab, consisting of Subject Matter Experts outside Government to act as an advisory body to the SDSC	Members of the SDSC	Chief Secretary, GoP	Chief Secretary, GoP

3 PSDP Project Management Unit (PMU)

The PSDP PMU will be based out of the DGRPG acting as the nodal body within it to dispense the functions of these guidelines. As established in Section 2.2.1, the *CDO with be the head of this Unit along with 3-5 support staff who will comprise of his/her office* (Refer to Section 3.2). For governance of Open Data, the main activities of the PSDP PMU would be to manage the State OGD Platform, provide Technical Advice to the departments, handhold for dataset contribution as well as capacity building of Data Contributors and Departmental Data Officers. For the Governance of Non-sharable/Personal Data the PSDP PMU will provide maintenance of the negative lists, technical advice to the Departmental Data Officers, the SDSC and maintain compliance with the PSDP, these guidelines and National level Personal Data Protection Regulations.

3.1 Roles and Responsibilities

3.1.1 Management of the State Open Government Data (OGD) Platform

The PSDP PMU will be responsible for management and hosting of the State OGD Platform from the DGRPG Headquarters adhering to these Guidelines and other National Level Government and Data security policies. The architecture of the State OGD Platform would be scalable and of high availability.

3.1.2 Technical Advice

The PSDP PMU will provide Departments with technical advice with respect to preparation of datasets, contribution of datasets, explanation of metadata and the entire workflow of data publishing, feedback management from departments complying with these guidelines, publishing Departmental Compliance Indexes based on the Maturity Model outlined (Refer to Section 11) and any other activity deemed necessary by the SDSC (Refer to Section 6.1 for guidelines on publication of datasets)

3.1.3 Capacity Building

Both as offsite and onsite training modules must be developed by the PSDP PMU. Each module would be for the duration of 2-3 days. The logistics and venue for the onsite training would be the responsibility of the host Department. The modules would be:

- **PSDP Awareness and Sensitization Module** – For the Departmental Data Officer & other senior officers of the Departments
- **Technical Modules on Data Contribution/Maintenance of Negative Lists/Data Exchange/Business Continuity** – Hands-on training for contributing datasets to the State OGD Platform, provide advisory on conversion of data to digital format to Data Contributors and Departmental Data Officers. Additionally, modules for Maintenance of Negative Lists, Data Exchange and Business Continuity will also be developed.

Please refer to Section 9 for guidelines on Training and Skill Development.

3.1.4 Maintaining Compliance with PSDP Guidelines and National level Personal Data Regulations

The PSDP PMU will be responsible for supporting the Departmental Data Cells of all Departments in maintaining compliance with these guidelines and other extant National level Personal/sensitive personal Data Regulations.

3.1.5 Management of Negative Lists

The PSDP PMU will be responsible providing support to the Departments for maintaining Negative Lists which have been notified. (Refer to Section 6.2 for notification of Negative Lists for the Government of Punjab).

3.2 Appointment of Support Staff for the PSDP PMU

In addition to the CDO, the SDSC will also appoint 3-5 Support Staff for dispensing the functions of the PMU. The support staff at the time of their appointments must have the following minimum qualifications:

- Bachelor's/Master's Degree in Information Management, Data Analytics, Computer Science, Program Management, Policy, Law, Economics, Statistics or a similar field
- At least 3 years' experience as a data specialist in a Government Department or a Multinational Firm
- Preferably prior experience in implementing Data Exchange Platforms for multinational firms or government bodies
- Ability to read, interpret, and verify data from multiple formats
- In-depth knowledge of data retrieval and storage systems
- Knowledge of computer hardware systems and peripherals
- Experience with end-user training and support

Special Focus on Immediate Responsibilities of the PSDP PMU
While the overall roles and responsibilities of the PSDP PMU has been mentioned in Section 3.1, post the establishment of the PMU, it will undertake full review of the current State OGD Platform to identify gaps and establish requirements based on this section and facilitate the development of the following modules, if not already present:
— Registration Based Data Publication/Validation System — ***System to be deemed available if it can:*** — Generate Log-In IDs for relevant personnel — Personnel can use provided Log-In ID to authenticate upload/verification of datasets on the State OGD Platform
— Staging Area Module within the State OGD Platform for uploaded datasets from Departments — ***System to be deemed available if it can:*** — Host departmentally uploaded datasets as an intermediary prior to final publication — Allow the PSDP PMU/CDO to view/verify departmentally uploaded datasets
— Registered Access Dataset Module within the State OGD Platform — ***System to be deemed available if it can:*** — Host semi-sensitive datasets with log-in requirement for access

— Provide Log-In IDs to specific personnel as deemed by the PSDP PMU to access semi-sensitive datasets — Host departmentally uploaded datasets as an intermediary prior to final publication — Allow the PSDP PMU/CDO to view/verify departmentally uploaded datasets
— Citizen Viewing and Feedback Module — ***System to be deemed available if it can:*** — Citizens can view open datasets without any prior end-user authentication and provide feedback on them — Citizen feedback is displayed to Departmental Data Cells for consideration
— Citizen Dataset Suggestion Module — ***System to be deemed available if it can:*** — Allow citizens to upload requests for new datasets — Suggestions are displayed to Departmental Data Cells for consideration
— Data Exchange Framework and Platform — Formulate Data Exchange Standards — Formulate API Standards — Formulate Predictive Service Suggestion System ***System to be deemed available if it can:*** — Operationalize Data Exchange between Departments and third parties incorporating Data Request, Evaluation, Impact Assessment and Risk Assessment guidelines mandated by these guidelines (Refer to Section 8)

3.3 Compliance Grid for Establishment of the PSDP PMU and its functions

Steps to be taken	Creator	Checker	Approver
Establishing/Revamping the State OGD Platform:			
Step 1: PSDP Project Management Unit to develop Registration Based Data Publication/Validation System	PSDP PMU	CDO	SDSC
Step 2: PSDP Project Management Unit to create Log-In IDs for Chief Data Officer, Departmental Data Officers and Departmental Data Cell Personnel to access and submit Open Access Datasets	PSDP PMU	CDO	SDSC
Step 3: PSDP Project Management Unit to develop Staging Area Module within the State OGD Platform for uploaded datasets from Departments	PSDP PMU	CDO	SDSC

Step 4: Establish Registered Access Dataset Module within the State Open Government Data Platform	PSDP PMU	CDO	SDSC
Step 5: Establish Citizen Viewing and Feedback Module	PSDP PMU	CDO	SDSC
Step 6: Establish Citizen Dataset Suggestion Module	PSDP PMU	CDO	SDSC
Step 7: Formulate Data Exchange Framework and Platform — Formulate Data Exchange Standards — Formulate API Standards — Create Policy Planning Tool — *Please also refer to Section 6 for detailed workflow of establishing this framework and platform*	PSDP PMU	CDO	SDSC
Publication of Open Datasets and Maintenance of Negative Lists: Please refer to Section 6, Compliance Grid			
Storage of Open Datasets and Personal/Sensitive Personal Data: Please refer to Section 7, Compliance Grid			
Training and Skill Development: Please refer to Section 9, Compliance Grid			
Review and Improvement of the PSDP and its guidelines: Please refer to Section 10, Compliance Grid			
Budgetary Allocation: Please refer to Section 11, Compliance Grid			

4 District Data Cells

As mandated by the PSDP, the SDSC will oversee the establishment of a District Data Cell in each district *under the chairpersonship of the Deputy Commissioner* to supervise, coordinate and ensure compliance to the PSDP and these guidelines at the district level as well as undertake practices for data digitization, management, processing, and analysis for evidence-based decision making.

The District Data Cell shall coordinate with the Departmental Data Cells as well as the CDO to ensure that all practices, as outlined under the PSDP and these guidelines, like those spearheaded by the CDO and/or the Departmental Data Officers are implemented in their respective districts.

4.1 Composition of the District Data Cell

Due to there already being an established Governance Structure being present at the district level, the charge of the ensuring compliance to the PSDP and these guidelines will be added to the Departmental Representatives at the District level. The Cell will be comprised of the following individuals:

- District Commissioner, Chairperson
- District Level Departmental PSDP Officers - The Departmental District level representatives will be given additional charge, e.g., the District Women & Child Protection Officer will be given charge of PSDP Compliance for the WCD Department at the District level
- District Level Data Entry Operator, to be nominated by the District Level Departmental Data Officers (Qualifications to be similar to the Subject Matter Experts at the PSDP PMU, refer to Section 3.2)
    - The District Level Departmental Data Entry Operator may hire external agents or third-party consultants for daily Data Entry to respective Departmental Portals/MIS

4.2 Roles and Responsibilities

The District Data Cell will be responsible for:

- Maintaining provisions of the PSDP and these guidelines during collection of personal/sensitive personal data at the field level for schemes
- Ensure regular entry of beneficiary information and linked Direct-Benefit Transfers into Departmental Portal/MIS
    - The Departmental MIS Systems will, ideally, be harmonized with Field level data standards notified by the PSDP PMU for data exchange, however, is not mandated (Refer to Operational Guidelines – Part 2, Section 4.1.2.6)
- Co-ordinating procurement and maintenance of IT hardware for the District Commissioners Office
- Facilitate overall technical/IT upgradation of the District Commissioners Office
- Maintaining adherence to reasonable security standards for personal/sensitive personal data storage as mandated by these guidelines[1]

[1] Ideally the Data Storage at the district level must also adhere to Reasonable Security Standards (Refer to Operational Guidelines – Part 2, Section 4.2.4.1), but given the current context, this is to be complied to as per the Maturity Model (Refer to Section 12)

- Facilitate transfer of all offline official/administrative documentation into digital form
- Training of District level Officers on overall aim and compliance requirements of the PSDP and these guidelines
- Training field level officers on usage of Departmental Portal/MIS
- Reporting to the District Commissioner for any anomalies to be brought to the attention of the PSDP PMU and SDSC for remedial action

4.3 Compliance Grid for Establishment of District Data Cells and its functions

Steps to be taken	Creator	Checker	Approver
Step 1: Deputy Commissioner to nominate District level Departmental Nodal Officers to dispose the functions of the District Data Cell	Deputy Commissioner	N/A	PSDP PMU
Step 2: District Data Cell to nominate District level Data Entry Operator, with provision for hiring of additional consultants, as and when needed	District Data Cell	N/A	Deputy Commissioner
Step 3: District Data Cell to develop IT procurement and maintenance plan for the building Data Entry Capacity	District Data Cell	N/A	Deputy Commissioner
Step 4: District Data Cell to develop Capacity building Plan for Data entry Operators on Departmental MIS Applications	District Data Cell	N/A	Deputy Commissioner
Additional Step: District Data Cell to submit report to District Commissioner in case of any breach of these guidelines to be brought to the notice of higher authorities	District Data Cell	N/A	Deputy Commissioner

5 Data Ethics Committee for Punjab

These guidelines mandate for the creation of a Data Ethics Committee within the DGRPG for ethical usage of data being captured by the Government of Punjab.

5.1 Committee Functions

The key prescribed functions of the Committee, will be to:

- To consider ethical matters relating to activities being conducted by the Owner Departments, including advising them on such matters; or imposing conditions, on ethical grounds, on the Department engaging in activities
- To advise Departments on ethical matters relating to the collection and production and re-production of beneficiary information and statistics
- Conduct Detailed Data Protection Impact Assessments (DPIA) for new schemes that are being undertaken by the departments involving the usage of beneficiary data (Refer to Operational Guidelines – Part 2, Section 4.2.4.3)
- All new schemes involving the usage of beneficiary information will be subject to approval by the ethics committee
- Further usage of beneficiary information by third parties under acceptable usage (Refer to Operational Guidelines – part 2, Section 4.2.3.5) will also be subject to review by the ethics committee for new projects
- Review proposals involving changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals, and therefore require a formal Privacy Impact Assessment
- Review applications for all new or amended data collections, for all projects that require use of identifiable data and projects requiring data linkage
- Review creation of new data collections and/or the acquisition of data collections from data suppliers
- Review changes in the nature or expanding the scope of existing data collections

5.1.1 Process for review

For any of the functions mentioned above, the owner Department will make a detailed representation to the Ethics Committee for review. Post the submission, the Committee will convene to either approve or send it back for revision. The Committee will convene on a priority basis or when 3 new approvals are pending on a staggered 15-day basis.

5.2 Ethical Standards

The Committee will adhere to the following standards while assessing ethical concerns related to the usage of beneficiary data:

- ‘Negligible risk usages’ describes usages in which there is no foreseeable risk of harm or discomfort; and any foreseeable risk is no more than inconvenience. This generally entails the use of existing collections of data or records that contain only non-identifiable data (Open Access Data) about human beings.
- ‘Low risk usages’ describes usages in which the only foreseeable risk is one of discomfort. This generally entails the usage of registered access datasets (Refer to Operational Guidelines – Part 2, Section 3.4). The parameters for designating an exercise as low risk are as follows:

- May lead to identification of a natural person/persons
- May lead to leakage data outside the borders of the state
- May lead to abuse/harm of children
- May lead to financial loss of natural person or the owner department
- May lead to data loss for the owner department

- "High risk usages" describes usages in which the risk for participants is more serious than discomfort and must be 'reviewed and approved by the Committee. This generally entails the usage of personal/sensitive personal data. Parameters for designating an exercise as high risk are as follows:
  - Requires raw beneficiary data with direct access to personal identifiers like address and other personal/sensitive personal data elements (Please refer to Operational Guidelines – Part 2, Section 3.3)
  - Has no time limit specified for the usage of personal/sensitive personal data
  - Data is to be transferred outside the Union of India

5.3 Constitution of the Committee

The Ethics Committee will be constituted of the following members:

- Principal Secretary, DGRPG (Chairperson)
- Principal Secretary, Department of Social Security, Women and Child Development
- Principal Secretary, Department of Legal and Legislative Affairs
- Principal Secretary, Department of Revenue
- Principal Secretary, Department of Planning
- Principal Secretary, Department of Information Technology
- Chief Data Officer, Government of Punjab
- Subject Matter Experts from the PSDP PMU
- Representative from the SDSC

The Deputy Secretary and the Director, DGRPG will be the joint conveners of the Committee.

5.4 Compliance Grid for Establishment of the Ethics Committee and its functions

Steps to be taken	Creator	Checker	Approver
Step 1: The SDSC to notify the establishment of the Data Ethics Committee with the mentioned members as its constituents	N/A	N/A	SDSC
Step 2: Ethics Committee to convene on a 15-day staggered basis for review of all new scheme/project proposals	Departmental Data Cells	PSDP PMU	Ethics Committee

6 Publication of Open Access Datasets and Notification of Negative Lists

This section is to be read in consonance with the guidelines for Data Governance Framework (Operational Guidelines - Part 2, Section 4). The PSDP PMU is responsible for the final upload of datasets on to the State OGD Platform and keeping an updated catalog of Negative Lists for the Government of Punjab. This section is to be undertaken by the PSDP PMU only after Departmental compliance to Data Governance Framework has been completed.

6.1 Publication of Datasets on the State Open Government data (OGD) Platform

Post uploading of datasets on the Staging Area Module by the Departmental Data Cells (Refer to Operational Guidelines – Part 2, Section 4.1.2.3), the PSDP PMU will forward the datasets to the CDO for approval. Further to approval, the PSDP PMU will push the datasets from staging area to the production area and publish it on the OGD Platform.

6.2 Notification of Negative Lists

The final Negative List for respective Departments will be forwarded to the PSDP PMU and the CDO for scrutiny. Post approval from the CDO, the Negative List will be notified as an official Negative List for the Government of Punjab by the PMU.

6.3 Compliance Grid on Final Publication of Datasets and maintenance of Negative Lists

Steps to be taken	Creator	Checker	Approver
Publication of the Datasets on the State OGD Platform:			
Step 1: Departmental Data Cells to upload datasets on the State Open Government Data Platform for review and publication by the PSDP Project Management Unit	Departmental Data Cell	PSDP PMU	CDO
Step 2: PSDP Project Management Unit to review submitted datasets in Staging Area Module for coherence with Open Data Publication Metadata Standards, Attribution Template Standards, Usage License Clarity and forward to Chief Data Officer for approval	PSDP PMU	CDO	N/A
Step 3: Chief Data Officer to approve publication of dataset or send them back for revision	CDO	N/A	N/A
Step 4: PSDP Project Management Unit to publish approved datasets on the State Open Government Data Platform	PSDP PMU	N/A	N/A

Notification of Negative Lists:			
Step 1: Review Departmental Negative Lists for coherence with personal/sensitive personal data identifiers mentioned	Departmental Data Cell	PSDP PMU	N/A
Step 2: Forward Negative Lists to the CDO for approval	PSDP PMU	CDO	CDO
Step 3: Notify Negative Lists as official Negative List for the Government of Punjab	PSDP PMU	N/A	N/A

7 Data Storage Guidelines

7.1 Overview

As mandated by Section 2, sub-section (17) of the PSDP, all departments must store their datasets at the State Data Centre. All 3 types of data, open, personal/sensitive personal, registered access will be kept within the State Data Center. The PSDP PMU will ensure that the State Data Center establishes standards *in coherence with the ISO/IEC 27001:2013 standards*, as mandated nationally by the IT Act (Privacy Rules) 2011 (refer to Annexure B for standards manual). Departments are allowed to store their data on another cloud technology service as a backup if required, given that it meets the standards mentioned in these guidelines.

7.2 Creation of Data Registers

As mandated by the PSDP, each department will create and maintain a single common comprehensive repository of its beneficiaries/users that will act as the single source of truth for the delivery of all services under the department to those beneficiaries/users. This shall be known as the 'Departmental Citizen Register'.

Each department will create and maintain a single comprehensive repository of its employees and all staff/workers engaged to work with the department temporarily or permanently, paid as well as unpaid. This shall be known as the 'Departmental Employees Register'.

Additionally, all departments shall be responsible to create and maintain data registers related to its specific operation and entity type. All other departments accessing such sector-specific data shall take these repositories as the single source of truth for that specific entity while using them for any transactional or service delivery purposes. *The standards for the creation of these registered will be formulated by the PSDP PMU. Further to that, the identification of key data points related to services for a specific Department for the purpose of these registers will be done by the Departmental Data Cells and ratified by the PSDP PMU.*

Some examples are given below:

- The Department of Industries and Commerce shall create and maintain a repository of all commercial as well as non-commercial enterprises registered in and/or operating in Punjab. This shall be known as the 'Business Register'.
- The Department of Revenue, Rehabilitation and Disaster Management shall create and maintain a repository of all land falling within the boundaries of Punjab. This shall be known as the 'Land Register'.
- The Department of Agriculture shall create and maintain a repository of all agricultural land and government run wholesale markets, falling within the boundaries of Punjab. This shall be known as the 'Agriculture Register'.

All departments must create these registers within 6 months of notification of these guidelines. More items under this list may be notified by the SDSC, as per requirement. All Registers will be updated every 60 days, after initial approval.

7.3 Current Status of the Punjab State Data Centre

The Government of Punjab currently operates a state-of-the-art State Data Centre and is certified by ISO 20000 & 27001 Information Management Standards. Due to the fact that the Reasonable Security Practices, mandated for the protection of personal and sensitive personal data also follow the same standards, Departments are allowed to store their beneficiary related personal/sensitive personal data in the State Data Centre.

7.4 Future Considerations

In the future, in case the any Department of the Government of Punjab develops the need for additional storage resources, the State is allowed to leverage the capabilities of existing commercial Internet Data Centers (IDCs) within the state for which different deployment models are available i.e., Co-located services, Dedicated Services and Managed Services.

Under this option, the State may identify a suitable model (confined to either co-located services or dedicated services only keeping in view the security implications) to select an appropriate agency through a suitable competitive process for outsourcing. The entire process of outsourcing, including advising on the most appropriate model, would be managed by the PSDP PMU.

Depending upon whatever outsourced model is selected by the State, Servers will be owned and operated by State and the management of the Data/Information shall be under the direct control of the State both de-jure and de-facto. For this, the State would require deploying a dedicated team which includes Project Manager (equivalent to Data Centre Manager), DBA, System administrator, Network Administrator, Support Staff etc., to be notified by the DGRPG, should the need arise.

7.5 Compliance Grid for Establishing Data Storage

Steps to be taken	Creator	Checker	Approver
Establishing Open/Registered Access Data Storage:			
Step 1: State Open Government Data Platform to be hosted from the State Data Centre - All datasets published on the State Open Government Data Platform will be hosted at the State Data Centre	Departmental Data Cells	PSDP PMU	CDO
Example: Establish "Government of Punjab Business Register" as the single source of truth for all commercial and non-commercial enterprises operating in Punjab - To be maintained by the Department of Industries, to be hosted from the SDC	Industries Department Data Cell	PSDP PMU	CDO
Establishing Personal/Sensitive Personal Data Storage:			
Step 1: Establish the "Punjab State Citizen Register" as the single source of truth of Beneficiary Information for all Departments, to be hosted at the SDC - Individual Department level Beneficiary Information will be maintained by the Department, to be hosted from the SDC	Departmental data Cells	PSDP PMU	CDO

Step 2: Establish the "Government of Punjab Employees Register" as the single source of truth for all government personnel, to be hosted from the SDC - To be maintained by the Department of Revenue, to be hosted from the SDC	Departmental Data Cells	PSDP PMU	CDO
Example: Establish the "Government of Punjab Land Register as the single source of truth for all land within the boundaries of the State	Revenue Department Data Cell	PSDP PMU	CDO
Future Expansion:			
Step 1: In case additional storage is required, the PSDP PMU to hire commercial Internet Data Centers, given they conform to the ISO/IEC 27001:2013 Security Standards - Additional Personnel needs to be hired by the DGRPG in this scenario	PSDP PMU	N/A	CDO

8 Data Exchange Guidelines

8.1 Data Exchange Framework

8.1.1 Overview

The PSDP 2020 aims to enable better information sharing and integration to support better decision-making, better value, and better services in a safe and secure IT environment. As part of achieving this, requires the development of a data exchange framework for the government. This action is supported by Section V, sub-section (4) and (5) of the PSDP.

These guidelines will create a standardized Data Exchange Framework for the Government of Punjab regardless of data type, classification, exchange method, platform, or intended use and users. It identifies the key steps and components of data exchange and the overarching governance and business rules.

The framework balances the need for privacy and legislative compliance with the need for better insights (informed decisions and evidence-based policy development), performance reporting and operational efficiency. It provides an authorizing environment to enable data exchange and sharing in day-to-day practice.

The framework supports the Government of Punjab's objectives of increasing access to government data by staff and systems and managing data holistically to remove duplication and gaps. These guidelines will form the basis on which an automated data exchange platform may be developed.

8.1.2 Defining Data Exchange

For the purpose of this framework 'data exchange' refers to exchanging or transferring data in a secure, authorized, and predefined way whether automated; real time or near real time; system to system; via secure file transfer; bulk uploads or once-off.

8.1.3 Objectives of this Framework

The objectives of the framework are to:

- Enable, encourage, and authorize data exchange to increase the value of the investment in government data and ease the sharing and/or integration of data between government (inter/intra department and agencies), third parties (managing information on behalf of government) and other jurisdictions.
- Reduce the cost and resource intensity of data exchange by creating a standardized Government of Punjab data exchange approach (regardless of data type, data exchange method or platform or intended use) and ensure responsibilities for the data after exchange are clear and agreed prior to exchange.
- Retain data integrity by considering the quality, value and authenticity of the data being exchanged.
- Balance the need for safety and transparency in data exchange with the need for better informed decisions, evidence-based policy development, performance reporting and operational efficiency.
- Ensure data exchanges are fit-for-purpose (i.e., meet business needs) and able to be supported.

8.1.4 Aim

This Data Exchange Guideline provides high-level advice to Government of Punjab, its associated departments, and other related agencies on evaluating, managing, authorizing, and undertaking data sharing. This guideline will assist Data Owner Departments and Data Requesting Departments to understand and implement the Data Exchange Standard along with the supporting tools and templates.

The guideline provides further advice and clarification on the minimum considerations that need to be considered in order to exchange data, the business rules that should be applied and use of tools to help in the assessment and management of data exchanges.

In this guideline, 'data' refers to structured data[2]. Unstructured data is not covered by this guideline.

Unless stated otherwise, all references to 'sensitive' data have the definition as provided in these guidelines.

8.1.5 Principles

The Government of Punjab Data Exchange Framework will be based on the following principles:

1	Transparent and collaborative accountability	Parties to a data exchange will collaboratively work together to ensure a secure, authorized, predefined and transparent data exchange. Roles and responsibilities for all parties involved in the data exchange are clearly defined and communicated. Data ownership and accountability throughout the data exchange process is understood.
2	Enabled exchange	Data from different sources is able to be exchanged and used appropriately. All data requests are managed and responded to within a timely and accommodating manner. Departments proactively seek and provide data via data exchange arrangements.
3	Authorized exchange	The authority (and approval) to exchange data is understood by all parties involved. Data privacy, confidentiality, security, and intellectual property is respected and protected during and after the exchange of data. Limitations to data exchange are understood, managed, and communicated. Data exchange business requirements are understood and applied. Data is exchanged with assurance provided for the appropriate use of data after the exchange

[2] Structured data' refers to data that can be organized and stored in fixed fields such as in a relational database record or spreadsheet. 'Unstructured data' does not conform neatly into a fixed field format. Examples include data streams, social media data, documents, emails, videos, audio files, and images.

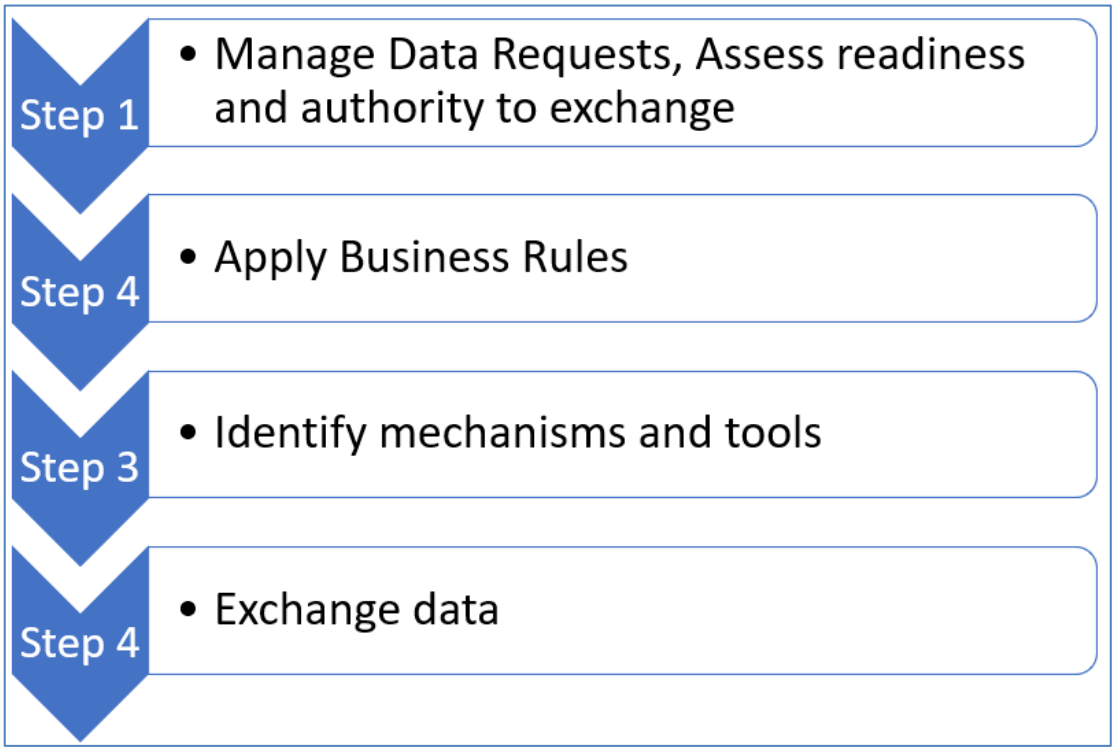
8.1.6 Scope

All departments within the Government of Punjab, are formally within the scope of these guidelines. While not required, the standard may be adopted by other agencies and partner organisations, working with the government.

8.2 Guidelines for developing a Data Exchange Model

The data exchange model developed articulates the journey from managing data requests, assessing readiness and right to exchange to carrying out the exchange of data. The framework provides a high-level overview of the data exchange process, its key components and the overarching governance and business rules. *It is a living record and high-level roadmap for the development of the key process components.* The components outlined in this section must be addressed for each step before operationalizing a data exchange.

The framework has been developed in consonance with the PSDP and existing national policies and guidelines and is aimed at creating one environment to support streamlined, safe and authorized data exchange.



8.2.1 Step 1 – Manage Data Requests, assess readiness and authority to exchange

Critical to successful data exchange or transfer is appropriately managing data requests (both requests received, and requests sent), assessing whether the data is ready to be shared and whether a department has the authority (the right) to share it. This is about enabling data exchange, ensuring that the exchange (or transfer) happens in a secure, transparent, and compliant manner and sufficiently describing the data and its quality to enable the data recipient to assess fitness for their intended purpose. It involves the following key components:

Sl. No.	Guideline	Description
1	Assess readiness to exchange	Outlines the parameters of readiness for data exchange including business value, associated risks, data protection, privacy impact assessments and de-identification, adequately described (metadata), data quality (data quality statements and the acknowledgement of data quality limitations) accessibility (particularly when the data resides in a legacy system) and systems (performance/load impacts and associated service levels) etc. Provides guidance on how to use these parameters to assess readiness, or lack of readiness, to exchange data.
2	Assess the right to exchange	Provides guidance on assessing whether a department has the right (authority) to exchange data (authorized release) including: • Legislative and administrative policy barriers - privacy, security, confidentiality, copyright, intellectual property rights • Associated risk to the department, government, and the public • Data exchange approval or consent (depending upon the criticality or risk associated with the data, use of the data or method of exchange) This guideline will also help the data owner to build the case for data exchange and assess whether the data exchange is in the best interest of the department, government, or the public. It will also consider if the data owner has the authority to withhold the data and the steps a requestor can take to appeal the decision to withhold.
3	Managing data requests	Guidance for making data requests and managing data requests received including: • Overarching governance including accountability, data ownership, roles, and responsibilities • What data is being requested and why • What to do when a request is received (review, assess and respond) • What to do when requesting data • The authorizing environment under which the data can be exchanged (see Assess readiness to exchange and assess the right to exchange) • Whether the request is once off or on-going, and the anticipated availability, volume, and frequency of the request

		• Understanding the business processes, scenarios or use cases for which the data will be exchanged • How to use the data request template

8.2.2 Step 2 – Apply Business Rules

Identification of business rules will help to ensure reliable, consistent, and sustainable data exchange and decision making. Knowing what a department can and cannot exchange, where accountability starts and finishes and how to protect the government as a result of the exchange etc. are all critical to successful data exchange outcomes. Departmental Business Rules will comprise of the following key components:

Sl. No.	Business Rules	Description
1	Data exchange standard/s	A series of standards identifying the business rules for data exchange: • Common schemas, patterns, and formats (metadata, common languages, comma separated, or tab delimited etc.) • Data dictionaries for common data types and schemas • Managing and exchanging common data types • Common data exchange methods including secure file transfer, API gateway, system to system, system to location, messaging services and data exchange services. Key consideration will be appropriate security based on the classification of the data being transferred and intended use • Consideration of what not to use when exchanging data i.e., email, CDs, unsecure cloud services etc.
2	Establishing a data exchange arrangement standard	Describes the minimum requirements when establishing a data exchange arrangement including: • What can be exchange/what cannot be exchanged • Legislative and administrative obligations • Data ownership and sovereignty; at which point does ownership transfer or not transfer • Roles and responsibilities i.e., ownership and accountability • Formalizing the arrangement including how to use the data exchange agreement or statement of intent including how to complete the associated data schedule • When to exchange without an agreement or statement • Licensing of data exchange arrangements • Cross-jurisdictional, inter and intra department, agencies, and third-party data exchange • Managing data exchange as a record

		• Managing risk and compliance including identifiable and sensitive data • Carrying out a privacy impact assessment of the data (both of the data to be exchanged and how it is intended to be used) • Lifecycle and change management i.e., establishing a refresh cycle for frequently changing data or data that has a time limit (e.g., annual datasets that expire on a certain data)

8.2.3 Step 3 – Identify mechanisms and Tools

Data exchange and transfer is an urgent need within the Government of Punjab, supported by a growing number of services and functions. Knowing what's available, who to talk to, and which tools and templates to use will support streamlined, safe, and authorized data exchange. Key components which make up exchange mechanisms and tools are as follows:

Sl. No.	Mechanisms & Tools	Description
1	Data services and infrastructure	Descriptions of and links to existing data services, data exchange services, platforms, and infrastructure within and external to government. For example, the existing State OGD Platform Tools, API gateways etc. Identification of future technical needs to facilitate data exchange.
2	Data sources and schemas	Descriptions of and links to existing data exchange schemas, design patterns and methods within the Government of Punjab and externally. Descriptions of and links to existing data sources, providers, registers/catalogues, and repositories including https://punjab.data.gov.in, internal information asset register, reference data, master data i.e., 'person', 'place' and 'economy' datasets etc.
3	Data experts	Links to expert groups within government who have responsibility for data exchange
4	Compliance	Descriptions of and links to legislative and administrative policies that impact data exchange including National level Legislations
5	Data exchange risk assessment model	The Data Exchange Risk Assessment Model will help assess the risk and apply appropriate controls to data exchange initiatives. This model will help data owners to assess if the data exchange is in the best interest of the government or of the public
6	Data request (template)	A template for data exchange requests including how the data requestor intends to use the data

7	Data exchange checklist (template)	A checklist that helps the data owner to assess the authority and justification for a data exchange arrangement. The emphasis of this checklist is not on preventing data exchange but rather on exchanging data in a safe (secure) and transparent manner
8	Data exchange agreement (template)	A standardized agreement/contract template for data exchange with third parties including service level agreement, change management and data schedule (a detailed description of the data)
9	Data exchange statement of intent (template)	A standardized data exchange statement of intent (or memorandum of understanding) template for inter and intra department data exchange including service level agreement and data schedule
10	Data exchange technical specification (template)	A template for documenting the technical specifications of a data exchange

8.2.4 Step 4 – Exchange Data

Each data exchange will differ in its characteristics but be similar in the process of designing, testing, and transitioning to streamlined operation. The following table outlines the key components on each stage of the process:

Sl. No.	Guideline	Description
1	Designing a data exchange	Guidance on the process of designing and carrying out a data exchange including: • Data exchange key concepts and terminology • The different types of data exchange methods e.g., system-to-system, SFTP, bulk upload versus single instances, real time versus near real time, large transactions, bulk uploads, and one-off or scheduled etc. • How to overcome the barriers to data exchange • The use of process flow diagrams, data architecture, modelling and mapping to support data exchange • Mapping interdependencies so there is an understanding of associated complexities • Data quality in the context of data exchange and links to a Data Quality Standard and associated toolset • Common and recurring schemas, patterns and methods for exchanging data including industry standards • Technology and data storage considerations • Usage considerations including data linkages, integration, and transformation

		• Contracts and service level agreement (SLA) considerations
2	Test a data exchange	Guidance on how to carry out end-to-end testing of a data exchange including: • Types of testing and when to use them • Common problems identified during data exchange testing • Identifying, documenting, and managing issues during testing • Data exchange validation and assessing the quality of the data received • Data handling and disposal during and after testing i.e., data security and preventing privacy breaches
3	Transition to streamlined operation	Minimum steps for handing over the data exchange arrangement to regular operations including exception handling, contract and SLA management, security, roles and responsibilities, asset management planning and maintaining data integrity, and ongoing monitoring and reporting, re-using exchanges, versioning and retiring

8.3 Data Exchange Standard

In addition to developing a data exchange model incorporating all components mentioned in Section 8.2, all Departments within the Government of Punjab must exchange[3] and share data in accordance with the requirements set out in this standard. Third parties or external agencies associated with the usage of Government Data will also need to adhere to the requirements of this standard.

8.3.1 Requirements

When exchanging data, departments must at a minimum:

Requestor (requesting department):

1. Include in a request for data:
    - The purpose and background context for the data request
    - A clear description of the data required
    - How the data will be used
    - Whether the data will be shared or distributed and to whom

[3] In this standard, 'exchange' is synonymous with sharing and refers to the one or two-way transfer of structured data in a secure, authorized, and predefined way, whether:

- Automated
- Real-time or near real-time
- System to system
- Via email
- Via secure file transfer
- Bulk uploads, ongoing or once-off
- Any other form of exchange not listed above e.g., flash drives

- Whether the request is once-off or on-going and under what conditions the data will be exchanged and managed

Provider (providing department):

2. Evaluate all data requests to assess whether the department has the right (or authority) to exchange the data requested including:
    - Legislative authority or obligation to share under legislation (Acts) relevant to the department or portfolio.
    - If the Provider is not the owner of the data, whether there is:
        i. A commercial agreement
        ii. Personal individual consent
        iii. Data asset owner's consent (if the data is owned by another department or agency)
3. Evaluate all data requests to assess whether the department is ready to exchange the data requested including:
    - Carrying out a risk assessment to determine risk to the department, the Government of Punjab and the public
    - Ensuring that where 'sensitive' data is involved, that a privacy impact assessment is conducted to ensure reasonable steps have been taken to protect the data from misuse or loss and unauthorised access, modification, or disclosure
    - Ensuing data is de-identified wherever possible, unless identified data is essential to enable the data to be fit-for-purpose
    - Assessing whether the Provider and the Requestor have the appropriate processes, technology and infrastructure in place, and sufficient capabilities and capacity to undertake the exchange
    - Whether the data is of sufficient quality to be fit-for-purpose, and if not, to provide appropriate disclaimers as to its use.
4. Disclose 'sensitive' information only to the extent required to meet the objectives of the request
5. Ensure that all data exchanges are accompanied by a data exchange arrangement - legally binding, non-legally binding or an Open Data license. The type of arrangement used should be based on who the department is exchanging data with, the level of data protection required, and the level of risk associated with the data and the data exchange
6. Ensure all legally binding and non-legally binding data exchange arrangements include these minimum requirements
7. Exchange data to the maximum extent possible under an Open Data license and release via http://punjab.data.gov.in as open data unless restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law

General:

8. Record all requests and data sharing arrangements into a register of data exchange initiatives for government probity and transparency
9. Ensure data exchange arrangements comply with the requirements for managing public sector data under these guidelines

10. Ensure all data exchanges are authorized by an officer of the Department at a level commensurate to the risk associated with the data and in accordance with the government's Policies and standards for government IT
11. Appoint an owner and custodian in each of the Requestor and Provider organisations who will be accountable and responsible for the data exchange

8.3.2 Parameters for when a Data Exchange Agreement is required

All data exchanges must be accompanied with a documented data arrangement. The type of arrangement (legally binding, non-legally binding or Open Data license) and format of the arrangement (formal or informal) will depend on who the data is being shared with i.e., internal, or external to the department, associated risk and level of data protection required. The following table outlines the kind of data agreements possible for nature of requests:

<table>
<tr><th rowspan="2">Requestor</th><th rowspan="2">Internal</th><th colspan="5">External</th></tr>
<tr><th colspan="3">Within the Government of Punjab</th><th colspan="2">Outside the Government of Punjab</th></tr>
<tr><td></td><td>Refers to requestors that are internal to the provider organizatio n (3)</td><td colspan="3">Refers to Government of Punjab departments and agencies. Note, while statutory bodies are part of the government, they are legal entities in their own right. A legally binding agreement should be entered into with a statutory body when warranted by the associated level of risk</td><td colspan="2">Refers to all other entities including government funded entities outside of government, local government, central government, governments in other jurisdictions and any non-government entities</td></tr>
<tr><td>Data risk</td><td>All levels (1)</td><td colspan="2">Not sensitive (1)</td><td>Sensitive</td><td>Not sensitiv e (1)</td><td>Sensitive</td></tr>
<tr><td>Arrangemen t type</td><td>Non-legally binding</td><td>Non-legally binding</td><td>Legally bindin g</td><td>Non-legally binding</td><td colspan="2">Legally binding</td></tr>
<tr><td>Format</td><td>Informal</td><td>Informa l</td><td>Formal</td><td>Formal</td><td>Formal</td><td>Formal</td></tr>
<tr><td>Example arrangement</td><td>Email</td><td>Email</td><td>License such as Open Data License (2)</td><td>Memorandu m or letter of understandin g (or other formal non-legally binding mechanism)</td><td>License such as Open Data License (2)</td><td>Legal Agreemen t</td></tr>
</table>

References

(1) If data is not 'sensitive', the Provider should consider releasing it as open data

(2) Refer to Open Data License (Please refer to Section 4.1.1.4)

(3) *For example, a requestor internal to the organization, Department of Social Security, Women and Child Development (DSSWCD) is a person within a branch or division of the DSSWCD. Other 'bodies' (agencies, statutory bodies, etc.) within the Government of Punjab, such as Department of Labour or Department of Sanitation are considered external to the organization of DSSWCD.*

8.3.3 Components to be included in a Data Exchange Agreement

The table below describes the minimum requirements for creating the different types of data sharing arrangements. These requirements are additional to standard terms and conditions found in a legal arrangement such as definitions, interpretations, compliance with laws, dispute resolution, variations, breach provisions and termination.

In the case of a formal arrangement (excluding licenses), if more than one dataset is to be exchanged with the same Requestor, it is recommended that general requirements that apply to any data exchange be captured in the terms of the arrangement and any specific requirements around datasets be captured in the schedules (i.e., each dataset should have its own schedule). The following checklist is to be used while deciding the components for a data exchange agreement:

Requirement	**Description**	**Arrangement type (Applicability)**		
		Non-legally binding		**Legally binding**
		Informal (e.g., email)	**Formal (e.g., MoU, LoU)**	**Formal (Legal Agreement)**
Purpose	The purpose of the initiative that underpins the data exchange, including the associated outputs, benefits, and outcomes to be achieved and how the data will be used to achieve these benefits and outcomes.	Yes	Yes	Yes
Background	Context around the initiative and the basis for the data exchange including relevant statutory powers, government policies, operational needs, and organisational strategic directives.	Yes	Yes	Yes
Period of agreement	Commencement date of the agreement, how long the agreement will	Yes	Yes	Yes

	be in place and / or the end date.			
Key contacts	Names, roles, and contact details of the appointed representatives of each party to the data exchange arrangement.	Yes	Yes	Yes
Obligations	The roles and responsibilities of each party, governance structures in relation to the arrangement and that all appropriate authorizations have been sought. This may include principles around data exchange.	Conditional (1)	Yes	Yes
Data description	Description of the data being exchanged, including data types, timeframes (e.g., data from 2010 – 2018, broken down by month), data-related standards used (e.g., metadata standards, GIS standards, industry standards), data security classification, whether the data has been de-identified, and the method used.	Yes	Yes	Yes
Terms of use and disclosure	How the data will be used, joined, or integrated, de-identified for privacy, reproduced, published internally, externally, or not at all, or commercialized. With whom may the Requestor share or distribute the data or outputs resulting from using the data and under what conditions this may occur.	Conditional (1)	Yes	Yes

Intellectual Property (IP) and licensing	Who has ownership of the data and IP rights? Who will own any new IP developed? Can the Requestor use the data for commercial purposes or building a brand or reputation and under what conditions? This may include an Open Data License and associated attribution.	No	Yes	Yes
Data quality statement	Details of the quality of the data. A data quality statement will be provided in the first instance and updated when there are changes to the any data quality dimensions, in accordance with the Best Practices Study.	Conditional (1)	Yes	Yes
Data exchange and management	How the data will be transmitted (methods and standards) by the Provider to the Requestor, how the data will be managed by the Requestor, including data security and privacy (including de-identification).	Yes	Yes	Yes
Service levels	Service levels around the provision of data including service availability and reliability targets, maintaining data quality (including de-identification of data), complaints handling process and response times and consequences of not meeting service level targets.	Conditional (2)	Conditional (2)	Conditional (2)
Change management	The process for managing changes to the data provided - what, how, who and when this is communicated from	No	Conditional (2)	Conditional (2)

	the Provider to the Requestor.			
Data retention / disposal	Relevant data retention periods and whether the data should be returned to the Provider or disposed of at the end of the retention period.	No	Yes	Yes
Breach in data use or disclosure	Outline the process for managing unauthorised use or disclosure of data and any sanctions for failure to comply.	Conditional (1)	Yes	Yes
Fees or charges	Outline any fees or charges that apply for providing the data and payment terms and conditions. This will apply only in certain circumstances.	No	No	Yes
Compliance	The Provider's rights to monitor compliance with the exchange standards and terms of the agreement.	No	No	Yes
Review of arrangement	If the arrangement is a rolling arrangement, there should be a date to review its ongoing effectiveness.	No	Conditional (2)	Conditional (2)
Schedules to the arrangement	A separate schedule should be provided for each dataset exchanged and should include the dataset name, description, data owner (or custodian), data fields, data definitions, data quality statement and data security classification.	No	Conditional (3)	Conditional (3)

References

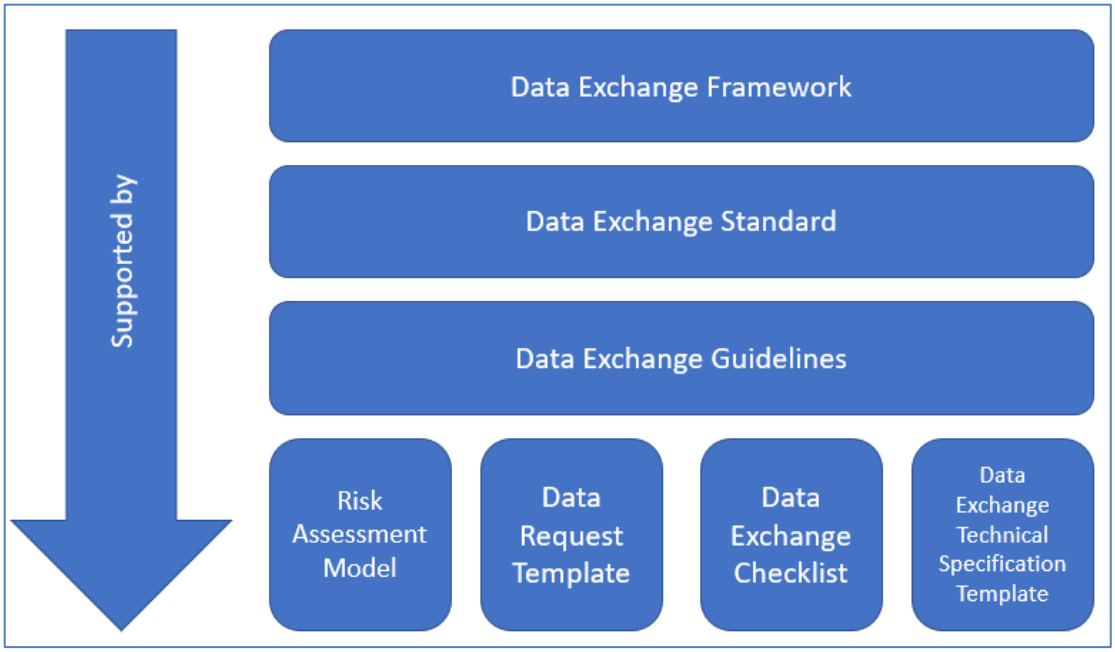
Conditional (1) Applies if personal or sensitive information or confidential data are involved

Conditional (2) Applies if data provision is recurring (i.e., not one-off)

Conditional (3) Applies if more than one dataset is exchanged

8.4 Guidelines for Implementation of the Data Exchange Framework and Standard

Implementation of the Framework along with the standard, risk assessment model, templates and checklists will follow this overall schema:



This guideline has been developed in alignment with the Data Exchange Standard and the guidelines for developing a Data Exchange Model:

Step 1: Manage data requests, assess readiness and authority to exchange

Step 2: Apply business rules

Step 3: Identity mechanisms and tools

Step 4: Exchange data

Departments will be seen as adhering to the standard, where they have processes in place which equal or exceed the requirements outlined in the subsequent sections.

8.4.1 Implementing Step 1 - Managing data requests, assess readiness and authority to exchange

8.4.1.1 Requesting data (Requestor)

The general process that a Requestor should follow to request for data involves five key steps:

1. Identify the need and purpose for data
2. Define the data you need
3. Determine if the data is already available as open data
4. Request for the data
5. Approve and submit the data request

A Data Request Template has been provided to demonstrate the key minimum requirements that should be covered when requesting for data. Additional information should be added into the request if it is relevant to strengthen the case for the request for data. This data

request template will be seeded into all data exchange models, irrespective of the type of exchange (offline/online) being pursued.

Data Request Considerations

When requesting for data, the Requestor should take into consideration all the elements outlined in following table. This will help the Requestor to not only provide a clear articulation of the data required, the purpose and use of the data, but also identify any gaps in the Requestor's ability to receive and manage the data in a manner commensurate to the risk involved.

Note that a lower level of detail may be provided in the data request form where the risk associated with the data is considered low. Data that is deemed medium to high risk will, by nature, require more information to ensure the Provider knows the exact purpose and use of the data and that the data will be secured and managed appropriately once it has been received. The Data request template (refer to Annexure A-5) has been developed adhering to the below mentioned considerations, however the following checklist must be cross-referenced by departments while requesting data:

Sl. No.	Area	Considerations
1	Purpose	What is the problem you are trying to solve or question you want answered? What is the name and objectives of the initiative you are undertaking? Does the initiative fall within a legislative requirement, or does it respond to a government policy, initiative, or directive? If so, provide details. What are the outputs, benefits, and outcomes of the initiative you are undertaking and to whom? What is the severity and magnitude of impact if you do not get the data you seek, and to whom?
2	Data description	Identify the data you need: • Data types (e.g., number of patients, by hospital, by location and average length of stay per patient) • Level of granularity of the data (unit record, aggregated) • Timeframe of data (e.g., data from 2010 to 2018, broken down by hourly intervals, by month and year) • 'Sensitive' data.
3	Source of data	Is the data you need already open and publicly available? • If so, use open data wherever possible • If not, identify who has the data you need • Additional information beyond what has been provided in the template can be added if required.

4	Use, sharing, distribution	How will the data be used? • Will the data be used to serve an operational function or be used in analysis for a particular initiative? • What are the use cases for the data? Will the data be joined or integrated with other data? • If so, what other data will be used? • What is the source of that other data? • How will all the data be used collectively? If it is known that the data requested contains 'sensitive' data that pertains to individuals or other entities such as businesses, and if it is required to be deidentified, how will the data be de-identified? • What de-identification method will be used? Who will use or access the data (e.g., contractors, analysts, consumers, executive management, board members, staff, and general public)? • Are they sufficiently skilled to use, handle and protect the data as required? Will the data or outputs from the use of the data be disclosed or published? • To whom: internal and or external parties? • How will confidentiality be maintained, if required? Are there any actual, potential, or perceived conflicts of interest in having access to or using the data, for the Requestor organization and individuals involved in the initiative?
5	Data exchange and management	What format is the data required to be in? How often do you need the data to be provided? • One-off • Recurring – near or real-time, daily, monthly, annually, etc. How do you want to receive the data? • Determine the required transmission method and standards. This may require a discussion with your Information Technology (IT) specialists if the transmission of data is to occur system-system or through another automated mechanism or require specific data exchange standard (language or format). How will the security, storage, access and disposal or deletion of the data be managed? • This should align with PSDP and these guidelines
6	Risks	If it is known that the data requested contains 'sensitive' data, what are the risks associated with receiving, managing, and using the data and what mitigations are in place?

		• Undertake a risk assessment (particularly around Safe People, Safe Settings, Safe Data and Safe Outputs) as described in the Risk assessment section • Mitigating any risks exposed from the assessment will improve the likelihood of the Provider approving the data exchange.
7	Request timeframe	By when is the data required? • What is the reason for this deadline?
8	Approval	The data request should be approved Departmental Data Officers. • As a guide, where the data requested is for data that is 'sensitive' in nature, the request should be authorized by the PSDP PMU

8.4.1.2 Evaluating a data request (the right and readiness to exchange) (Provider)

The general process that a Provider should follow to evaluate a data request is involves three key steps:

Assessing the right to exchange:

- Determine whether the Provider has the right or authority to exchange the data

Assessing the readiness to exchange:

- Undertake a risk assessment and privacy impact assessment (if applicable)
- Determine if the Requestor and Provider are enabled (have the data, appropriate technology, infrastructure, policies, and processes) to undertake the exchange and securely manage the data (readiness to exchange).

Considerations when evaluating a Data request:

A Data Exchange Request Evaluation Checklist has been provided to highlight the key considerations that should be covered when evaluating a data request. The following table outlines the considerations that should be taken into account while evaluating a data request:

Sl. No.	Area	Considerations

1	Right or authority to share	Is the request for 'sensitive' data?
		Does the Provider have the right or authority to share the data under?
		• Legislative authority or obligation to share under legislation (Acts) relevant to the department or portfolio
		• If the Provider is not the owner of the data, whether there is:
		  ◦ a commercial agreement,
		  ◦ personal individual consent or
		  ◦ other department data asset owner's consent (if the data is owned by another department or agency)
		that permits the exchange of data (noting that permission to exchange may only be for certain limited purposes).

		If the request is for 'sensitive' data and the Provider does not have the right or authority to share it, the Provider could negotiate with the Requestor to provide deidentified data. If the Provider does not have the authority or right to share the data, the Provider should issue a response to the Requestor in writing stating the reason for not providing the data and referencing any relevant legislation or policies that prohibited the exchange.
2	Risk assessment	The key steps in assessing risk are: • Determine the Provider's risk appetite for data sharing • Undertake a risk assessment for the data request • If the data request is for personal data, a Privacy Impact Assessment should also be undertaken • Decide whether the risk justifies the benefit for sharing the data If the Provider deems that the risk and mitigations do not outweigh the benefits of sharing the data, the Provider should issue a response to the Requestor in writing stating the reason for not providing the data, referencing any policies that prohibit the exchange.
3	Source of data	Is the data you need already open and publicly available? • If so, use open data wherever possible • If not, identify who has the data you need
4	Enabled Exchange	Does the Requestor have the appropriate technology, infrastructure, policies, and processes to undertake the exchange and securely manage the data? This can be determined via the risk assessment of Safe People, Safe Settings, Safe Data and Safe Outputs If gaps are identified, the Provider should inform the Requestor of the gaps and the required mitigations. The Requestor may choose not to proceed with the mitigations and forego the request, at which point the process ends. Is the Provider enabled to exchange the data? **Access to data** • Is the data easy to access and extract from the system it resides in? • Is the impact on the system when extracting the data significant enough to cause performance issues? If so, how will this be mitigated? **De-identification** • Will de-identification of the data be required? If so, what method will be used? • How will de-identification, and maintaining the privacy of the individual, be managed, and maintained if the data provision is recurring?

		Process • Is there an existing data exchange process? If not, a process will need to be created • Are all participants in the process aware of their roles and responsibilities and the rules of the exchange? • How will errors, faults, recovery and complaints be handled and monitored? **Data Quality** Less than perfect data quality, alone, should not be a barrier to exchange data, however it is up to the Provider to determine whether the data quality renders the data fit-for-purpose. • Is the Provider enabled to supply a data quality statement? o The Provider should issue an updated statement if changes in the data impact the data quality. **Metadata** Is the Provider enabled to supply metadata? If so, what metadata standard will be used? Updated metadata should be provided if changes occur. **Capacity** Does the Provider have the capacity to undertake the exchange within the timeframe and ongoing if the data provision is recurring? ▪ A lack of or limited capacity, of itself, should not be considered as a reason not to undertake the exchange, but rather a factor that may impact the scope and or timing of the exchange.

8.4.1.3 Risk Assessment Model

A risk-based approach to the data request evaluation is recommended, which aims to balance the risk of disclosure with the proposed benefits and outcomes of the initiative being undertaken by the Requestor.

The evaluation process involves undertaking a risk assessment using a risk assessment model (risk model) that incorporates the Five Safes Framework[4], reputational risk, and public risk, visualized here:

Incorporating the Five Safes Framework, the following table outlines the components that should be evaluated when doing a risk assessment for a data exchange:

Sl. No.	Component	Description
1	SAFE PROJECTS	**Is this use of the data appropriate?** • Refers to the legal, moral, and ethical considerations surrounding the use of the data. • Are the objectives, outputs, benefits, and outcomes of the initiative reasonable and in alignment with the purpose and functions of the Requestor organization? • What are the risks of loss, harm or detrimental impact to the department, individuals, wider government, general

[4] The Five Safes is a framework for helping make decisions about making effective use of data which is confidential or sensitive. It is mainly used to describe or design research access to statistical data held by government agencies, and by data archives such as the UK Data Service, Eurostat and Statistics New Zealand. Two of the Five Safes refer to statistical disclosure control, and so the Five Safes is usually used to contrast statistical and non-statistical controls when comparing data management options.

		public of sharing (or not sharing) the data? Are there any mitigations? This should be described in the section in the data request around the purpose for the request, the objectives, outputs, anticipated outcomes, and benefits of the initiative.
2	SAFE PEOPLE	**Is the user authorized to access and use the data?** • Refers to the knowledge, skills and incentives of the users using the data. • Is the Requestor organization reputable and trustworthy? • Do the staff possess the knowledge (e.g., skills and experience) to effectively use the requested data for the proposed purpose? How will the Provider or Requestor ensure that their staff have appropriate and sufficient knowledge? • What are the roles and responsibilities for all the staff (or user groups) who will have access to the data and what level of access will they have? This should be described in the section in the data request around who will have access to the data and how they will use the data.
3	SAFE SETTINGS	**Does the access environment prevent unauthorised use?** • Refers to the controls on the way the data is accessed, including physical, procedural and compliance controls. • Does the Requestor possess the technical requirements (e.g., equipment, software), governance, policies, and processes to effectively manage and enable the use of the requested data for the proposed purpose? • Where will the data be stored and used? • What security and technical safeguards are in place to ensure data remains secure and protected from unauthorised access and use (e.g., governance, physical safeguards, personnel, and cyber security arrangements)? Safeguards must align with the classification of the data being shared • How will the data be dealt with after it has been used for this purpose? This should be described in the section in the data request on how data will be managed.
4	SAFE DATA	**Has appropriate and sufficient protection been applied to the data?** • Refers to whether the data itself contains sufficient information for confidentiality to be breached? • Is 'sensitive' data requested? Is the data required to remain identified?

		• If not, the Provider should ensure that the data is de-identified. • If identified data is required, the Requestor should outline how they will deidentify the data and ensure that confidentiality is maintained • If the data is going to be joined or integrated with other datasets, how will this happen and how will the resulting data be used? Does this increase the risk of disclosure? • Are there any potential data quality, matching, reconfiguration, interpretation, or other issues regarding the data being requested? This should be described in the section in the data request on how the data will be managed.
5	SAFE OUTPUTS	**Are the analytical results non-disclosive i.e., individuals or groups cannot be re-identified from the outputs from the initiative?** • This is the final check on the information before it is released which aims to reduce the risk of disclosure to a minimum • Will the results of the data or analytics work on the shared data be published or disclosed? If so, what is the nature of the proposed publication or disclosure? • Who will be the audience for the publication or disclosure? • What is the likelihood and the extent to which the publication or disclosure may contribute to the unauthorised identification of a person in the data? This should be described in the section in the data request on how the data will used and managed.
6	REPUTATIONAL RISK	**Refers to whether there are any:** • Threats or danger to the good name or standing of the department • Risk that the outputs or results of the initiative could contradict or refute any government-wide policy or directive This can be ascertained by reviewing the purpose of the request, how the data will be used and who the audience for the outputs of the initiative.
7	PUBLIC RISK	**Refers to whether there are any risks to the safety, security and or wellbeing of the general public.** This can be ascertained by reviewing the purpose of the request, how the data will be used and who the audience for the outputs of the initiative.

The general process that a Requestor should follow in assessing the risk of a data exchange involves four key steps:

- Check Departmental risk appetite
- Undertake the risk assessment
- Evaluate the data exchange risk against the risk appetite
- Develop a risk management strategy (if required)

When assessing the risks of a data exchange, the following should be taken into consideration:

<table>
<tr><th>Sl. No.</th><th>Area</th><th>Considerations</th></tr>
<tr><td>1</td><td>Departmental risk appetite</td><td>What is the departmental risk appetite for data exchange?
Prior to undertaking the risk assessment, a check needs to be made against the organisational risk appetite. The risk appetite is the level of risk (high, moderate, or low) the organization is willing to accept around all data exchanges and is the benchmark to compare the risk of the particular data exchange. Should a risk appetite not exist, assume a ‘moderate’ level.</td></tr>
<tr><td>2</td><td>Risk assessment</td><td>What are the data exchange risks?
Risk assessment entails reviewing each of the risk components (the Five Safes, reputational and public risk) and assessing the consequences of each risk component
The overall risk of the data exchange should be based on the risk component with the highest risk rating</td></tr>
<tr><td>3</td><td>Risk evaluation</td><td>How does the overall data exchange risk compare to the departmental risk appetite?
Risk evaluation involves comparing the data exchange risk rating against the departmental risk appetite. If a risk appetite for data exchange cannot be determined, a ‘moderate’ risk appetite can be assumed.
The process of evaluating risk is:
Compare the overall data exchange risk against the Department’s risk appetite. The mapping below shows the relationship between the risk appetite and corresponding maximum level of data exchange risk:<table><tr><th>Organisational risk appetite</th><th>Data Exchange risk rating</th></tr><tr><td>Low</td><td>Significant or High</td></tr><tr><td>Moderate</td><td>Moderate</td></tr><tr><td>High</td><td>Low</td></tr></table>
If the data exchange risk is Significant or High and risk appetite is Moderate or Low, then a risk management strategy needs to be prepared and approved by Departmental Data Cells</td></tr>
<tr><td>4</td><td>Risk management strategy</td><td>Where a risk management strategy is required, it must contain risk mitigation treatments to either avoid or reduce the risk to an acceptable level.</td></tr>
</table>

		The risk management strategy should contain: • *The risk and the risk level* • *The risk control and treatments to reduce the risk, including timelines* • *The people responsible for executing the actions* • *The owner of the risk and the risk management strategy* • *Monitoring requirements for the risk* • *Applicable reviews of the risk and risk management strategy*
5	Executive approval	The final risk management strategy must be approved Departmental Data Officer of the Provider Department.

Risk assessment is composed of two parts:

- **Assessing the risk consequence** – Identifying the consequence (impact) of the data exchange against the seven risk components
- **Assessing the risk likelihood** – Assessing each risk component and consequence for the likelihood (probability) of the risk occurring

Using the review of the risk components:

- Assess the potential consequences and likelihood of each component using the risk consequence table and the risk rating matrix to determine the risk rating
- Identify the component(s) with the highest risk rating. This will be used to represent the overall risk rating for the data exchange in the risk evaluation stage of the risk assessment

The following chart shows the method of assigning risk ratings to data exchange requests with the following table highlighting the significance and fallouts of each rating:

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood ▼	Rating	1	2	3	4	5
Almost Certain	5	Medium	Medium	Significant	High	High
Likely	4	Low	Medium	Significant	Significant	High
Neutral	3	Low	Medium	Medium	Significant	Significant
Unlikely	2	Low	Low	Medium	Medium	Medium
Rare	1	Low	Low	Low	Low	Medium

Consequence Rating				
Insignificant – 1	**Minor – 2**	**Moderate – 3**	**Major – 4**	**Catastrophic – 5**
Safe Projects				
No identified ethical aspects	Having minor ethical risks	Having ethical risks which	Having identifiable	Clear ethical risks, or using

or not using data involving people	which can be mitigated, or using highly aggregated or obfuscated data which has no residual personal information	require monitoring, or using lightly aggregated or obfuscated data with a possible risk of reidentification of individual information	ethical risks which require significant attention, or using lightly aggregated or obfuscated data with a plausible risk of reidentification of individual information	personal information without appropriate deidentification or security controls
Safe People				
Authorized people interacting with the data have the knowledge and skills for required management and use of the data	Authorized people interacting with the data have reasonable knowledge and skills for required management and use of the data	Authorized people interacting with the data have minimal knowledge and skills for required management and use of the data	Authorized people interacting with the data have little to no knowledge and skills for required management and use of the data	Unauthorised management or use of the data
Safe data				
No sensitive data requiring treatment	Unauthorised disclosure of sensitive data to an internal party	Unauthorised disclosure of sensitive data to a single external party (not including the general public)	Unauthorised disclosure of sensitive data to multiple external parties (not including the general public)	Unauthorised disclosure of sensitive data to the general public
Safe Settings				
System accessed with multi-factor user authentication, active action logging, full audit trail of data lifecycle, anomaly detection, prevention of on-sharing	System accessed with multi-factor user authentication, user action logging, prevention of on-sharing	System accessed with multi-factor user authentication, no ability to readily on-share	System accessed with named user login authentication, limited ability to on-share	System accessed with no restriction on who can access data with ability to on-share

Safe Outputs				
Projects based on open data or projects considered to be Highly Safe.	Projects based on low value data or projects which are considered to be Safe	Projects based on moderate value data or projects which are considered to have a Moderate Level of Safety	Projects based on high value data or projects which are considered to have a Low Level of Safety	Projects based on very high value data or projects which are considered Not Safe
Reputational Risk				
Minor, adverse local public or media attention or complaints	Media attention of local concern	Significant adverse attention by media and or public	Serious public or media outcry (State coverage)	Serious public or media outcry (National coverage)
Public Risk				
No public risk to wellbeing or safety or members of the public identified	Minor public risk to wellbeing or safety. Potential for a person to be identified	Significant public risk to wellbeing or safety. Potential for a person to be identified	Major public risk to wellbeing or safety or members of the public identified	Serious public risk to wellbeing or safety or members of the public identified

8.4.2 Implementing Step 2 - Applying the business rules

8.4.2.1 Data exchange arrangement (Requestor and Provider)

The general process that a Provider and Requestor should follow to negotiate and agree on a data exchange arrangement should involves three key steps:

- Select an appropriate arrangement tool
- Negotiate the terms and conditions of the arrangement
- Obtain approval and sign off for the arrangement

Arrangements come in many variations and range by type (legally or non-legally binding) and by format (informal or formal). The selection of arrangement should follow the rules set out in Section 8.2.2 and Section 8.2.3.

When entering into a data exchange arrangement, the Provider and Requestor should take into account the following considerations:

Sl. No.	Area	Considerations
1	Arrangement selection	Data should be made available under the Open Data License to the maximum extent possible, unless restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law.

		The main considerations in selecting the appropriate type of arrangement are: • Whether the Requestor is internal or external to the department • The risk associated with the data, as determined via the risk assessment. The higher the risk the more formal the data exchange arrangement should be. Refer to Section 8.2.2 and 8.2.3 for various types and formats of arrangements and rules on how to select the appropriate one
2	Negotiate the arrangement	Section 8.2.3 outlines the minimum requirements for a legally or non-legally binding arrangement (excluding Open Data license), depending on whether the request is internal or external to the department. **Obligations of parties** The arrangement should outline the responsibilities of each party as well as any governance or oversight body (e.g., steering committee) created as part of the arrangement. **Data description** The data description should include: • Types of data - dimensions (e.g., dates, locations, age groups, other subject specific categories) and measures (e.g., count of people, amount of expenditure, average age, expenditure) • Timeframe of the data (e.g., data from 2010 – 2018, broken down by month) • Data-related standards used (e.g., metadata standard, GIS standard) • Data security classification applied • If data has been de-identified, what method was used? • Refer to Section 8.4.2.2 for the Data Exchange Technical Considerations and Annexure A-7 for Data Exchange Technical Specification Template **Terms of use and disclosure** • For what purpose(s) can the data be used? • Is Requestor permitted to join or integrate the data with other datasets? If so, which datasets and their sources? • Is the Requestor required to de-identify the data? • Is the Requestor permitted to reproduce, distribute, or published the data or outputs of the initiative internally or externally? If so, to whom and under what conditions? • Does the Provider want the right to review the outputs before it is published?

		• Is the Requestor permitted to commercialize the data? **Intellectual Property (IP) and licensing** Who will own any new IP developed? It is quite common for Requestors to join or integrate the data provided with data from other sources and create new datasets. The arrangement should address the ownership of the new datasets. • Does the Requestor require consent from the Provider on how, when and who can use this new data set? • Does the Provider want the right to review the output before it is published by the Requestor? **Data exchange and management** This section should cover: • How the data will be transmitted by the Provider to the Requestor • How the data will be managed by the Requestor. <u>Data transmission (Provider)</u> • Format of the exchange - the format in which the data will be provided (e.g., CSV, XLSX, DB, API) • Frequency of transmission – one-off, recurring (how frequently?) • What method of transmission will be used (e.g., system-to-system, bulk upload, web portal transfer, via email, via encrypted flash drive)? • Whether encryption of the data is required • Refer to Section 8.4.2.2 for the Data Exchange Technical Considerations and Annexure A-7 for Data Exchange Technical Specification Template. <u>Data management (Requestor)</u> • Where the data will be stored • Who will have access to the data? • If required, how will data de-identification and confidentiality be maintained • How the data security will be maintained over access and use of the data • Whether the data will need to be disposed of or returned to the Provider after the term of use • Refer to Section 8.4.2.2 for the Data Exchange Technical Considerations and Annexure A-7 for Data Exchange Technical Specification Template **Service levels**

		• This section outlines the Provider's responsibilities in providing the data: • When the data will be provided (e.g., within 3 days after month end) • If the data transmitted via an automated mechanism (e.g., system-to-system, bulk upload, API), the level of reliability and availability of the mechanism ○ Refer to Section 8.4.2.2 for the Data Exchange Technical Considerations and Annexure A-7 for Data Exchange Technical Specification Template • Maintenance of data quality to the level specified in the data quality statement • Provision and maintenance of metadata • What are the consequences if there is a failure of service • Complaint handling • Resolution timeframes **Change management** The Provider's responsibility to notify the Requestor if: • Changes occur that impact data quality or format. The elements of data quality are described in Annexure • Changes occur to the metadata When and how will the notification occur? When will the updated data quality statement or metadata be provided?
3	Obtain sign off	The arrangement should be approved or signed off by an officer from each party with the appropriate level of authority in accordance with their respective information governance, delegation of authority or security policy.

8.4.2.2 Data exchange technical considerations

When exchanging data, the Provider and Requestor will need to take into account technical considerations around the data, its transmission and management. A Data Exchange Technical Specification Template (refer to Annexure A-7) has been provided as an example of what technical details should be supplied to the Requestor when the data is exchanged, in addition to the data quality statement and the metadata document.

It is recommended that this document be completed by both the Provider and Requestor (in the relevant sections indicated in the template) in consultation with their Departmental Data Cells.

The technical considerations are as follows:

Sl. No.	Area	Considerations

1	Data (Provider, unless stated otherwise)	Document the data schema and model (structure of the data, variables, data types, interdependencies, mappings, and process flows) Definitions of the data (data dictionary) to aid interpretation and understanding of the data. e.g., "X" Region is a geographical area in Punjab where services are provided (definition). Regions comprise four areas: North (define boundary), South (define boundary), East (define boundary) and West (define boundary). Metadata standard used in providing the metadata document What is the data security classification of the data? Data must be classified to ensure appropriate security is applied during the exchange. Data should be classified in accordance with the PSDP and these guidelines.
2	Transmission (Provider, unless stated otherwise)	Will the data be exchanged once, or will there be on ongoing process? Where there is an ongoing process, how frequently will the exchange occur? The frequency of the exchange should be an input into the technical design of the exchange. What is the size or volume of the dataset to be exchanged? If the exchange is recurring, how will the size or volume of data change over time? Will the dataset be exchanged as a batch or incrementally as it is generated? The size of the dataset and batch vs. incremental transmission should be an input into the technical design of the exchange. For example, a large dataset that is to be transferred as a batch may not be suited to an API or messaging style of transfer. Consideration should be given to reliable file transmission methods such as SFTP. The transmission method used should be appropriate for: • The frequency of the exchange • The size or volume of the data that will be exchanged during each exchange instance • Whether the exchange will be batch or incremental • The security classification and level of risk of the data. The higher the risk, the more secure the method required. Example transmission methods include: • Secure file transfer using protocols such as Secure File Transfer Protocol (SFTP), File Transfer Protocol Secure (FTPS) or Hypertext Transfer Protocol Secure (HTTPS)

		• Application programming interface (API) such as the government's API Gateway • System-to-system • System to location • Messaging • Bulk uploads • Email • External storage media such as flash drives, CD or DVD. While there is no definitive guide for when a particular transmission method should be used, the following rules should typically apply: • Frequent exchanges with smaller data volumes may be more suited to automated, machine methods such as APIs • Large data volumes may be more suited to file transfer mechanisms such as SFTP • Sensitive data should never be transmitted via email or external storage devices The format or language that will be used to transfer the data, such as: • CSV, comma separated file • TXT, plain text file • XML, type of open data format • JSON, JavaScript Object Notation • Standard Interchange Format • Data Interchange Format • Open Document Format. Will encryption be required? If so, what encryption method will be used? Any encryption applied must be done so using an appropriate method. Both the Provider and Requestor need to ensure that the data: • Can be provided via the agreed transmission method • Can be received via the agreed transmission method • Can be read in order to extract the data for use.
3	Management (Provider and Requestor)	(Provider) Will there be a performance impact to the source system due to the extraction and or transmission of the data? (Requestor) Will there be a performance impact to the target system due to the receipt and or transmission of the data? Has adequate testing been carried out to understand the impact?

		If there is a potential impact, how will this impact be mitigated? (e.g., transfer outside of business hours) (Requestor) How and where will data be stored once it is received? • Is there sufficient storage capacity to store the data files, especially when the data exchange is ongoing and involves large data files? • Will the data be encrypted where it is stored? • How will the data be disposed of if the Requestor will only retain it for a limited time? (Requestor) How will data be secured once it is received? • Are there adequate security controls in place to ensure it is protected from unauthorised access, modification, and loss? • How will access to the data be restricted? • What level of access (read or write) will the permitted users (or groups) be given? • What is the technical process where there is an interruption or fault within the data exchange? The process should consider: • Monitoring for errors and faults • Ability to restart the process while ensuring no data is lost and no duplicates are produced.

8.4.3 Implementing Step 3 – Identifying mechanisms and tools

The guidelines outlined in Step 1 to 2 involves multiple considerations to be taken care of while implementation. To ease the implementation, the following mechanisms and tools have been developed in accordance with these guidelines which can be referenced while implementing a data exchange. The following checklist outlines the tools that have been provided which must be seeded into all data exchange modalities developed by the Government of Punjab:

Sl. No.	Area	Mechanism or Tool
1	Data request	**Data Request Template** Contains all minimum considerations that should be addressed in a data request.
2	Data request evaluation	**Data Exchange Request Evaluation Checklist** An example of the key considerations that should be addressed when evaluating a data request. **Risk Assessment Model (Please refer to Section 8.4.1.3)** Helps to assess the risk and apply appropriate controls to data exchange. This model will help data owners to assess if the

		data exchange is in the best interest of the either the Provider or Requestor departments, the wider government or of the public
3	Data exchange	**Data Exchange Technical Specification Template** Contains all technical details that should supplied to the Requestor when the data is exchanged. **Data Quality Statement Template** An example of the key information about data quality that should be supplied to the Requestor when exchanging data.

8.4.4 Implementing Step 4 – Exchanging the Data

The general process that a Provider should follow to undertake a data exchange arrangement involves three key steps:

- Design and implement the data exchange
- Test the data exchange
- Operationalise the data exchange

8.4.4.1 Data exchange design and implementation

Many of the design and implementation considerations have already been discussed in the evaluation (Section 8.4.1.2), arrangement and technical considerations (Section 8.4.2.2). The following table incorporates all the already mentioned elements in addition to other considerations. The Provider and Requestor columns indicate which considerations are relevant to each party:

Sl. No.	Area	Considerations	Provider	Requestor
1	Data exchange governance and authorization	Identify the data exchange owner and custodian for the data exchange transaction. • The owner will be accountable and have the power to authorize the exchange • The custodian will be the contract manager and the main operational point of contact for the exchange.	**Yes**	**Yes**
		Organisations quite often do not share their data for various reasons that usually stem from actual or perceived risk of negative consequences. It is important to remember that the government endorses an open data policy on public data wherever possible. Undertaking a risk assessment and identifying and mitigating risk gaps may	**Yes**	**N/A**

		help to alleviate the concerns for exchanging data.		

2	Enable the exchange	Do both the Provider and Requestor have the appropriate technology, infrastructure, policies, and processes to undertake the exchange and securely manage the data?
		This is discussed in greater detail in:
		• Section 8.3.1
		  • Access to the source data
		  • Data de-identification
		  • Processes
		  • Data quality
		  • Metadata
		  • Capacity and resources
		• Safe People, Safe Settings and Safe Data sections of the risk assessment in Section 8.3.1
		• Technical considerations in Section 8.4.2.2
		Data models, schemas, dictionaries, metadata
		• De-identification methodology
		• Transmission method and format
		• Data management including storage, retention, and disposal
		• Security and confidentiality
			Yes	**Yes**

		Artefacts that document the data exchange should be maintained and shared with the Requestor to help aid understanding of the data. These artefacts should include: • Data Quality statement • Metadata document • Technical specification document	**Yes** **Yes** **Yes**	**N/A** **N/A** **Yes**
		Internal artefacts that document the exchange should be maintained include: • Data exchange register • Data exchange policies, data models, schemas, and process flows	**Yes** **Yes**	**Yes** **Yes**

		• Risk register (in relation to data-related risks)	**Yes**	**Yes**
3	Agree on an arrangement	The terms and conditions for the data exchange should be captured in a data exchange arrangement. Both parties will have responsibilities around how the data is transmitted, managed, and used. The considerations outlined in Section 8.3.2 and Section 8.3.3 should be addressed.	**Yes**	**Yes**
4	Operationalise the exchange	What are the service levels required to be maintained in providing the data? This will inform the development of the arrangement. Refer to the service levels in Section 8.4.2.1	**Yes**	**N/A**
		What is the process to manage changes to the data that impact data quality and metadata? Refer to Change management in Section 8.4.2.1	**Yes**	**N/A**
		How will the Provider monitor that the Requestor is complying with the conditions of the arrangement, especially with regard to how they manage and use the data? How will the Requestor demonstrate to the Provider that they are in compliance with the conditions of the arrangement?	**Yes** **N/A**	**N/A** **Yes**

8.4.4.2 Data Exchange Testing

Testing is an essential part of the data exchange process. It will highlight any issues in the data, process, or systems (for both the Provider and Requestor) that need to be addressed and potentially altered in order to ensure a successful operational data exchange.

Testing should be designed and implemented in consultation with Departmental Data Cells of both Provider and Requestor Departments to ensure it is carried out correctly. The key considerations when testing a data exchange are outlined below:

Sl. No.	Area	Considerations
1	Designing the testing process	When designing the testing process, all parts of the exchange should be considered including the business process, system and data components. It may be appropriate to conduct testing within a dedicated testing environment where:

		• The complexity of the exchange is high or
		• There is an impact to current production systems.
		
		The test environment should be an exact replica of the production environment, ensuring issues that would appear in production will be visible in the test environment.
		
		Testing may not be required for all components and should be performed to an appropriate level.
		
		• What is considered 'appropriate' will depend on multiple factors that include but are not limited to:
		  • The complexity of the exchange
		  • The frequency of the exchange
		  • The level of automation involved in the exchange
		  • The risk associated with the exchange e.g., the higher the risk the more testing required
		  • The security classification and sensitivity of the data
		
		For example, a frequently occurring, fully automated exchange will require comprehensive testing of all components of the process.
		
		One off transfers of a single file, however, may not require detailed testing of the technical exchange component however:
		
		• Validation of the data may still need to occur to ensure that it is of the agreed structure and format and of an appropriate level of data quality.
		• The supporting business process should still be considered and tested.
		
		The test process should have a clearly documented test plan that defines what testing will be performed, how, when and by whom.
		
		The test plan should also document how defects or issues will be documented, tracked, managed, and resolved.
		
		Where detailed testing of the technical process and or validation of the data is required, it may be necessary to define and document the individual test cases that are to be carried out.
		
		A range of tests should be considered when designing the testing process. While the tests that are appropriate is highly dependent on the scenario and risk, some example tests that may be carried out include:
		
		• End-to-end testing
		  • Does executing the end-to-end exchange process produce the expected result?
		  • Has the data been delivered to the specified location?

		• Does executing the end-to-end exchange process complete without errors?
		Is the supporting business process robust?
		• Data protection / security
		  • Has the data been de-identified where required?
		  • Has the data been encrypted during transmission if required?
		• Validation of data
		  • Is data being received as per the agreed schema and format?
		  • Is all data present?
		  • Does all data conform to any agreed business rules and required transformation?
		• Performance testing
		  • Does the data exchange occur within acceptable performance limits?
		  • Is the time to transmit the data acceptable?
		  • Is the load placed on the source system acceptable?
		  • Is the load placed on the receiving system acceptable?
		• Access
		  • Is access allowed to the data for those with the appropriate privileges and blocked for those without at the receiver end?
		• Fault tolerance and resiliency
		  • Can mid-exchange failures be recovered from?
		  • Is appropriate logging in place so a failure can be investigated?
		  • What notification process is in place to notify relevant stakeholders?

2	Executing the testing process	Testing should be conducted until all defects or issues have been resolved, or there is agreement between both the Provider and Requestor that a defect can remain (i.e., the impact of the defect is low). As testing is cyclical and will require input from both the Provider and Requestor, it is important that agreement is reached on resourcing and scheduling from both parties. It is generally preferable to conduct testing with both synthetic data (made up to test the known boundaries of the process) and actual data. Whether it is necessary to use synthetic data in the testing process should be considered as part of design.

		Where the actual data to be transferred has a high security classification or is considered 'sensitive', it may be necessary to conduct testing with purely synthetic data. In this situation, it is extremely important that the synthetic data is representative of the actual data that will be transferred in the exchange. The use of automated testing tools and utilities should be considered for more complex data exchanges. Automated testing can help reduce testing timeframes in certain scenarios such as: • Where test cases need to be executed a large number of times • Where changes are expected to be made to the data exchange process over its lifetime and ongoing, repeatable testing is required after each release. Automated testing is not appropriate for all data exchange scenarios and the following should be considered: • An initial development overhead is required to set up automated testing • Automated testing usually requires specialized development resources.
3	Managing the testing process	Tracking and managing issues and defects Defects and issues should be logged in a register that is accessible by all parties involved in the testing process. It is recommended that a specialized defect or issue management tool is used for this register where one is available. Any actual (real) data used during the testing process should be handled according to the agreed access constraints and secured using approved security controls. This may include: • Encrypting data at rest and in transit where required • Restricting access to data from unauthorised individuals • Permanently deleting data at the conclusion of testing

8.4.4.3 Operationalizing the data exchange

Operationalizing a data exchange (where it becomes part of a streamlined operation) occurs when the exchange of the actual (real, not test) data occurs. This may occur as a one-off or recurring process. The key considerations when operationalizing a data exchange are outlined in the following table, unless otherwise stated, these considerations apply to both one-off as well as recurring data exchanges:

Sl. No.	Area	Considerations	Provider	Requestor
1	Change management (only applicable to recurring data exchanges)	Changes may occur from time to time that impact data quality (such as the way data is collected, how dimensions are defined, how measures are calculated, data stops being collected) or impact the format or method of the exchange. • If the changes impact data quality, the Provider should update and reissue the data quality statement to inform the Requestor of the changes • If the changes impact metadata, the Provider should update the metadata and inform the Requestor of the update • If changes impact the format or method of the exchange, the Provider should work with the Requestor to test the new format or method • Change management should be addressed as part of the data agreement arrangement • Notification of changes should be within the timeframe set out in the arrangement or at least when the next tranche of data is provided.	**Yes**	**N/A**
2	Exception handling	Exception handling is required when there is a failure in the data exchange process. This can happen at any point of the process, from data collation to transmission. An example is when system outages (such as source systems of the data, data distribution portals) occur that delay the provision of the data: • The Provider should consider how the failure is going to be remediated • Exception handling (including complaints handling) should be addressed as part of the arrangement in the service levels section.	**Yes**	**N/A**

3	Contract management (including service levels)	As part of the arrangement, both parties should appoint a data exchange owner and custodian. • The owner will be accountable and have the power to authorize or stop the exchange, if required • The custodian will be the contract manager and the main operational point of contact for the exchange The custodian should monitor each party's obligations as set out in the arrangement and manage issues if they arise. This may include: Monitoring and reporting performance against the obligations (such as service levels) Ensuring changes and exceptions (see above) are managed Liaising with the other party to resolve any issues Monitoring changes to the terms and conditions of the arrangement and amending the arrangement where necessary Renegotiating or extending the contract, if required. Complex, high risk data exchanges may need a regular face to face status meeting.	**Yes**	**Yes**
4	Monitoring and reporting	As part of contract management, custodians will need to be able to monitor each party's obligations of the arrangement. This may require reviewing or updating various reports such as: • Monitoring log reports of when data is provided to ensure data is provided within the timeframe set out in the arrangement • Monitoring log reports of when data is accessed and by whom to ensure data is only accessed by permitted users • Monitoring system error log reports to identifying system failures • Updating the data exchange register for the data exchange(s)	**N/A** **N/A** **Yes** **Yes** **Yes**	**Yes** **Yes** **Yes** **Yes** **Yes**

		• Monitoring data exchange risks and updating the risk register • Monitoring the sharing, management, and security of the data in accordance with these guidelines • Where applicable, reviewing the output to ensure deidentification has occurred If and when required, ensuring the data is returned to the Provider or disposed of in an appropriate manner in accordance with the arrangement.	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**

5	Resourcing	Do all the people involved in the data exchange understand their roles and responsibilities?
		• The roles that may be involved in an exchange are listed below. The roles do not always have to be held by different people. An individual may sometimes have multiple roles:
		  • Data exchange owner
		  • Data exchange custodian
		  • Information management specialists
		  • Information technology specialists (security, ETL, data warehousing, testing)
		  • Data analysts (analysts, researchers)
		  • Data consumers (internal: business managers, general staff, external: other public sector, private sector, special interest groups, general public)
		Do all the people involved in the data exchange have sufficient knowledge and skills to manage and or use the data for its intended purpose?
		If not, education and training may be required to be provided
			Yes
			Yes
				Yes
				Yes

8.4.5 Compliance Grid for Establishment of Data Exchange Platform

Steps to be taken	Creator	Checker	Approver
Step 1: Establish Data Exchange Framework based on Principles outlined in the Guidelines	PSDP PMU	CDO	CDO
Step 2: Operationalise Data Exchange with the following steps: - Exchange Request - Request Evaluation - Risk Evaluation - Exchange Agreement - Technical Specification Harmonization	PSDP PMU	CDO	CDO
Step 4: Establish usage of provided templates for data exchange	PSDP PMU	CDO	CDO

Creating subsequent Open Application Programming Interface[5] (API) based e-Governance System

The parameters laid down by the Data Exchange Guidelines will be used for the development of a Punjab Open API e-Governance System which will be an Open API-based e-Governance system aimed at creating a State Data Highway and ultimately integrate it with a National Data Highway. This will allow all State Government Services to be digitally accessible to citizens through multiple channels, such as web, mobile and common service centers. The PSDP PMU will notify the following sub-policies to these guidelines, as per the maturity model:

- Open API Principles
- High-level Architecture
- Service-level Architecture
- API Specification/Standards Template

[5] API – An Application Programming Interface (API) can be defined as a set of programming code that enables data transmission between one software product and another. It also contains the terms of this data exchange. Application programming interfaces consist of two components:

- Technical specification describing the data exchange options between solutions with the specification done in the form of a request for processing and data delivery protocols
- Software interface written to the specification that represents it

9 Training and Skill Development Guidelines

9.1 Background

Alongside a strong IT infrastructure, governance framework and guidelines for data governance, it is crucial that government manpower is regularly upskilled on technical skills, practices and know-how of data handling, management and use such that the PSDP may be successfully implemented, and data may be used to its potential for evidence-based decision making. Training and skill development shall be designed to equip all government manpower with the appropriate and up-to-date knowledge and skill sets such that a culture of data-driven governance is encouraged and adopted by all in the Government of Punjab. As per the provisions of the PSDP:

- The SDSC, in consultation with the Expert Group, shall lay down a plan for regular training and skill development of all government manpower, especially the manpower involved in data collection, processing, management and/or use
- Under the guidance of the SDSC, the DGRPG and Department of Planning shall develop training modules which shall be made available online and can be used by all officials and staff engaged in data collection, management, processing and/or use to enhance their skills on the matter
- The Department of Planning shall develop, make available, maintain, and regularly update content on data governance including data handling, management, and use
- The DGRPG shall develop, make available, maintain, and regularly update content on the IT infrastructure and protocols used for data collection, processing, management, and use
- The DGRPG shall also build a common platform where this content can be accessed and used by all government officials and staff

9.2 Establishment of PSDP Workshop Requirements (periodic)

- Further to the notification of these guidelines the PSDP PMU will conduct Implementation Workshops every 3 months for each department
- The Workshops will happen in a staggered manner, with multiple sessions on each topic for the relevant people from the Departments to attend

9.3 Training Modules

- The PSDP PMU will establish modules based on all sections of these guidelines for instruction at the PSDP Workshops
- These modules will be disseminated digitally to every department
- The modules will be regularly updated

9.4 Compliance Grid for Training and Skill Development

Steps to be taken	Creator	Checker	Approver
Step 1: The PSDP Project Management Unit in consultation with the State Data Steering Committee to prepare plan for 1-year Training Workshops (1 every 3 months)	PSDP PMU	CDO	CDO

Step 2: PSDP Project Management Unit to prepare Awareness and Sensitization Modules for Chief Data Officer, Departmental Data Officers	PSDP PMU	CDO	CDO
Step 3: PSDP Project Management Unit to prepare Data Collection, Contribution, Processing, Publication, Storage, and Redressal Modules for Departmental PSDP Data Cells based on the Guidelines and the PSDP	PSDP PMU	CDO	CDO
Step 4: PSDP PMU to host all modules in online form on the State OGD Platform	PSDP PMU	CDO	CDO

10 Review and Improvement Guidelines

10.1 Background

Similar to the PSDP Policy itself, these guidelines will be reviewed by the SDSC in coordination with the Expert Group, at least once every 2 years to update and revise the policy as may be required in accordance with the applicable laws, infrastructure, and other developments.

10.2 Third-party assessment of policy implementation and practices

As has been mentioned under Section V (5), the Chairman of the SDSC under the guidance Departmental Data Officers under the guidance of their respective Administrative Secretaries shall actively build collaborations with external organizations for third party audit and assessment of datasets generated from information being entered into the MIS; guidelines being used to process and use the datasets under the MIS; and the MIS being used by each department/agency. Such assessments are recommended to be done once every year.

10.3 Compliance Grid for Review and Improvement

Steps to be taken	Creator	Checker	Approver
Review of Regulatory Structure:			
The State Data Steering Committee to conduct review of the PSDP Policy and its Guidelines every 2 years	PSDP PMU	CDO	SDSC
Review of Departmental Technical Capabilities:			
The PSDP Project Management Unit to conduct review of Departmental MIS Systems and State OGD Platform and Data Exchange Platform on a yearly basis	PSDP PMU	CDO	SDSC

11 Budgetary Allocation Guidelines

The implementation of Punjab State Data Policy is expected to entail expenditures for both data owners and data managers for data conversion, data refinement, data storage, quality upgradation, etc.

The administrative departments/public organizations may approach the Department of Finance for appropriate budget allocation in this regard.

11.1 Key components for Budgetary Allocation

The PSDP Implementation Budget should take into consideration the new products, and services, necessary to layer the PSDP and its guidelines on top of, or modify, existing data sources and associated operations/processes.

Key allocation components that must be accounted for are:

- Governance
    - Establishing Sate Level Implementation Authorities and associated roles
    - Establishing Department Level Implementation Authorities and associated roles
    - Establishing District Level Implementation Authorities and associated roles
- Citizen Interaction and Grievance Redressal
    - Establishing citizen interaction personnel for the State OGD Platform
    - Establishing Legal Representation for Departments during grievance redressal
- Information Technology (Hardware and Software)
    - Reviewing established modules and implementing new mandated modules for the State OGD Platform
    - Procurement of SDSC and PSDP PMU IT Hardware requirements
    - Procurement of Departmental Data Cell IT Hardware Requirements
    - Procurement of District Data Cell level IT Hardware Requirements
    - Development of Open API e-Governance System
    - Development of Departmental MIS/Portals for state-run schemes
    - Development, maintenance, and expansion of data storage requirements
- Conducting Training Workshops
    - SDSC, PSDP PMU level training requirements
    - Department level training requirements
    - District level training requirements
- Business Continuity
    - Emergency funds for implementing system continuity in cases of natural disaster and other exigencies

11.2 Compliance Grid for Budgetary Allocation

Steps to be taken	Creator	Checker	Approver
Step 1: Departmental PSDP Data Cells to prepare full expenditure requirements and submit it to the PSDP Project Management Unit of the DGRPG	PSDP PMU	CDO	SDSC
Step 2: The DGRPG to seek requisite Budget from the Department of Finance, Government of Punjab based on estimates provided by the Department	PSDP PMU	CDO	SDSC
Step 3: Further to budgetary allocation, the DGRPG to allocate resources to Departments in consultation with the State Data Steering Committee and the Data Experts Group	PSDP PMU	CDO	SDSC

12 PSDP Implementation Maturity Model

The following Maturity Model will be used to gauge the Government of Punjab's compliance level to the PSDP and these guidelines:

Outcome	Compliance Level	To be Completed by
1. Establishment of Implementation Authorities as mandated by these guidelines	10%	1st Year
2. Identification and Classification of Data as mandated by these guidelines	20%	1st Year
3. Notification of data standards for field level data elements	30%	1st Year
4. Complying to Data Governance Framework as mandated by these guidelines	40%	2nd Year
5. Complying to Data Storage Requirements as per these guidelines **- Notification and Implementation of the ISO/IEC 27001:2013 information management standards**	50%	2nd Year
6. Establishing Departmental MIS/Portals	60%	2nd Year
7. Complying to Data Exchange Framework as mandated by these guidelines **- Interim offline/online implementation of the 4-step data exchange methodology**	70%	2nd Year
8. Shift to and development of Open API e-Governance System based on the Data Exchange Framework	80%	3rd Year

- **Notification of API Standards** - **Operationalization of system**		
9. Notification of Business Continuity/IT Recovery Plan - **State level** - **Department level** - **District level**	90%	3rd Year
10. Establishment of an Efficient Service Delivery System	100%	3rd Year
11. Establishment of Training Modules and Workshops	N/A	As required

13 Organogram for Implementation Authorities