प्रधान महालेखाकार (ले0&ह0) का
कार्यालय
बीरचंद पटेल पथ,
पटना, बिहार – 800001

OFFICE OF THE PRINCIPAL
ACCOUNTANT GENERAL (A&E),
BIRCHAND PATEL PATH
PATNA, BIHAR - 800001

SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

O.O. No.: DACell/2026-27/03
Dated: 27/05/2026

कार्यालय आदेश

Pursuant to Headquarters' directions received vide mail dated 19.05.2026 and in compliance with the Data Governance and Data Security Policy (August 2024) of the CAG of India along with the provisions of the Digital Personal Data Protection (DPDP) Act, 2023, the Pr. Accountant General (A&E), Bihar, Patna has nominated the following officers/officials and constituted the **Data Security and Governance Group of this office,** as detail below:

Sl No.	Profile	Name Shri	Designation
01	Data protection Officer	D P Srivastava	DAG (Works, Accounts & VLC)
02	DPDP Officer	Jitendra Kumar Sinha	Data Manager/VLC
03	DPDP Officer	Manish Kumar	Data manager/ITS
04	IT infrastructure management	Sunny Prakash	AAO/ITS
05	IT infrastructure management	Abhishek Kumar	AAO/ITS
06	Cyber security	Shakti Kumar	AAO/GIA
07	Cyber security	Mantoo Kumar Sinha	AAO/VLC

Further, the headquarters office vide its another mail dt. 19.05.2026 has provided with Standard Operating Procedure (SoP) on secure Data Sharing in IA&AD which is shared with this office order to all the nominated members of the Data Security and Governance Group for strict compliance with the Hqrs' instruction in matters relating to data sharing and governance.

Digitally signed by DEVENDRA PRATAP SRIVASTAVA
Date: 27.05.2026 12:39:10

Dy. Accountant General
(Accounts, VLC and Works)

Copy forwarded for information and necessary action to:

1. Secretary to the Pr. Accountant General (A&E), Bihar, Patna.
2. PA to DAG (Works, Accounts & VLC).
3. PA to Sr. DAG (Admin)
4. PA to Sr. DAG (Pension)
5. All nominated Officers/Officials of the Data Security & Governance Group.
6. Sr. AO/ITS Cell (with a request to upload the order on the office website).

Sd/-

Sr. Accounts Officer
Data Analytics Cell

Fwd: [Cag-all-offices] Standard Operating Procedures for Data Sharing

AG AE Bihar Patna < agaebihar@cag.gov.in >

Tue, 19 May 2026 1:36:31 PM +0530

To "Record section"<record.bih.ae@cag.gov.in>

Cc "Santosh Kumar CAG"<kumars@cag.gov.in>,"Lokesh Datal" <lokeshdatal@cag.gov.in>,"Omnkar K"<omnkar@cag.gov.in>,"Devendra Pratap Srivastava"<srivastavadp@cag.gov.in>

O/o the Principal Accountant General (A&E), Bihar, Patna
Veerchand Patel Path, R. Block
Patna-800001

========== Forwarded message ==========
From: B K Mohanty <mohantybk@cag.gov.in>
To: "cag-all-offices"<cag-all-offices@lsmgr.nic.in>
Cc: "Surjith K"<surjithk@cag.gov.in>, "Ajay Yeshwanth"<ajayyeshwanth@cag.gov.in>, "Chandersheel"<aao1cdma@cag.gov.in>
Date: Tue, 19 May 2026 12:53:42 +0530
Subject: [Cag-all-offices] Standard Operating Procedures for Data Sharing
========== Forwarded message ==========

All Heads of Field Offices,

The Standard Operating Procedure (SoP) on Secure Data Sharing in IA&AD has been finalised and is attached herewith for strict compliance.

2. The SoP is being issued in alignment with the Policy on Data Governance and Data Security and the provisions of the Digital Personal Data Protection Act, 2023. It lays down a structured framework for data request, classification, approval, sharing and handling, with clearly defined roles of Data Owners, DPOs and CDPO.

3. It is reiterated that:

(i) All data requests shall be processed strictly through the prescribed Annexure (attached) and no data shall be accessed or shared without due approval.

(ii) Sharing of Sensitive Personal Information and Negative List data shall require prior approval of the Chief Data Protection Officer (CDPO), in this case DG (IS).

(iii) Data sharing shall be strictly on a need-to-know basis and through secure, authorised channels only.

(iv) Data retention, archival and deletion shall be carried out strictly in accordance with approved timelines and applicable rules.

4. All HODs in Field Audit and Accounts Offices are requested to:

(a) Disseminate the SoP to all concerned officials and field parties;
(b) Ensure active involvement of DPOs in all data and cyber security related matters;
(c) Put in place necessary internal controls and monitoring mechanisms for compliance; and
(d) Maintain proper audit trail of all data sharing transactions.

5. Instances of data breach or non-compliance shall be reported immediately to this office and the CISO/CDPO.

B K Mohanty
ADAI & CTO cum CDPO

1 Attachment(s)

Data Sharing - SoP.pdf
226.2 KB

STANDARD OPERATING PROCEDURE (SoP) - SECURE DATA SHARING (IA&AD)[i]

1. Introduction:

This Standard Operating Procedure (SoP) is issued under the overall guidance of the Chief Technology Officer (CTO), who is responsible for prescribing data access rules and periodically reviewing existing controls to strengthen data protection measures across the IA&AD as per 4.3(i) of Policy on Data Governance and Data Security.

2. Scope:

2.1. Applicable to:

2.1.1. Data sharing between **CDMA (HQ)** and **Field Offices**

2.1.2. Data sharing between **Field Offices**

2.1.3. Data sharing between **Field Offices** and **Auditee Units**

2.2. Covers:

2.2.1. ***Negative List*:** as per 2.12 of Policy on Data Governance and Data Security

2.2.2. ***Personal Data*:** as per 2.13 of Policy on Data Governance and Data Security

2.2.3. ***Sensitive Personal Information (SPI)*:** as per 2.16 of Policy on Data Governance and Data Security

2.2.4. ***Shareable data:*** as per 2.15 of Policy on Data Governance and Data Security

2.3. Key Functionary involved:

2.3.1. ***Chief Technology Officer (CTO): as*** per 4.3(i) of Policy on Data Governance and Data Security

2.3.2. ***Chief Data Protection Officer (CDPO):*** as per 2.2, 4.3(d) and 4.3(h) of Policy on Data Governance and Data Security

2.3.3. ***Data Protection Officer (DPO):*** as per 2.7, 4.3(e), 4.3(f) and 4.3(g) of Policy on Data Governance and Data Security

2.3.4. ***Data Owner:*** as per 2.8, 4.3(a), 4.3(b) and 4.3(c) of Policy on Data Governance and Data Security

3. Methodology for Data Request, Sharing and Retention

3.1. Data request shall be initiated by the requesting office through the prescribed Annexure, clearly specifying purpose, dataset and retention requirement; no access to data shall be assumed or exercised at this stage.

3.2. The request shall be routed to the data providing office, where the Data Protection Officer (DPO) shall examine the request for necessity, proportionality and purpose limitation *(refer Sections 4.3(g)(i), 4.6)*.

3.3. The classification of data (Shareable / Personal Data / Sensitive Personal Information / Negative List) shall be determined solely by the data providing office based on policy provisions *(refer Sections 2.12, 2.13, 2.15, 2.16, 5(2))*.

3.4. The request, along with DPO recommendations, shall be placed before the Data Owner for approval. In cases involving Sensitive Personal Information or Negative List data, prior approval of the Chief Data Protection Officer (CDPO) shall be obtained *(refer Sections 4.3(b), 4.4, 4.6(ii))*.

3.5. No data shall be shared without completion of the above approval process *(refer Sections 4.3(b), 4.6(ii))*.

3.6. Upon approval, the providing office shall prepare the dataset strictly limited to the approved scope and ensure that only necessary and permissible data is included *(refer Sections 4.5, 4.6(i))*.

3.7. Data shall be transmitted through authorised secure channels, duly encrypted and access-controlled, and transfer details shall be recorded in the Annexure *(refer Section 6(i), 6(iv))*.

3.8. The receiving office shall access the data only through authorised systems and strictly for the approved purpose; further sharing or duplication shall not be permitted without fresh approval *(refer Sections 4.3(b)(ii), 6(x))*.

3.9. The receiving DPO shall ensure controlled usage, maintain audit trail of access, and enforce compliance with data security requirements *(refer Sections 4.3(g)(iii), 6(v))*.

3.10. The DPO of the requesting office shall assess the extent of data to be shared with the field parties or other concerned persons for processing of the data and prescribe appropriate safeguards, including data minimisation, masking or anonymisation, wherever required *(refer Section 4.5 and 4.6 (i))*.

3.11. Data retention shall be limited to the period approved in the request or as per applicable rules, whichever is earlier, and shall be governed by the Data Owner *(refer Section 4.3(b)(iii), 6(xii))*.

3.12. Upon completion of the intended use, the receiving office shall ensure secure archival or deletion of data, and certify disposal in accordance with prescribed procedures *(refer Section 6(vii))*.

3.13. Storage of data on personal or unauthorised devices shall be avoided, and any temporary storage shall be purged after transfer to designated systems *(refer Sections 6(vii), 6(viii))*.

3.14. All data sharing transactions shall be logged and periodically reviewed by the DPO to ensure compliance with the Data Governance and Data Security Policy *(refer Sections 4.3(g)(vii), 6(iii))*.

3.15. Any breach or deviation shall be immediately reported to the HoD and CDPO, and necessary corrective action shall be initiated *(refer Section 4.3(g)(viii))*.

Annexure-I: Data Sharing Form

Section-A: Requesting Office

1. General Information*

- **Date of Request:** _____
- **Requesting Office:** _____
- **Division/Section:** _____
- **Name & Designation of Officer:** _____
- **Official Email ID:** _____

2. Dataset Details*

- **Name of Dataset(s):** _____
- **Time Period Covered:** _____
- **Ministry/Department Data pertains to:** _____

3. Purpose and Justification*

a) **Purpose of Data Request:**

_____

b) **Specific Use Case (Audit/Analysis/Research):**

c) **Justification (Why data is required):**

_____

4. Data Security and Handling Assurance (By Requesting DPO)

- Data will be:
  - Used strictly for stated purpose
  - Stored only in authorised systems
  - Not shared further without approval
  - Archived or Deleted as per extant rules and provisions after the purpose mentioned in 3(b) above is fulfilled.
- **Retention Period Requested:** _____
- **Undertaking by Requesting Officer:**
  "I undertake to comply with IA&AD Data Governance Policy and DPDP Act provisions."
- **Signature:** _____
- **Name:** _____

Section-B: Data Providing Office

5. Approval Section

a) Type of Data Requested (Tick as applicable)*:

☐ Shareable Data
☐ Personal Data
☐ Sensitive Personal Information (SPI)
☐ Negative List Data

b) Data Owner Approval (by DPO)*:

- Approved / Rejected
- Remarks/Conditions (if any): _____
- Name & Signature: _____
- Date: _____

c) CDPO Approval (if applicable):

- Required for SPI / Negative List
- Approved / Rejected
- Conditions: _____
- **Name & Signature:** _____
- **Date:** _____

6. Data Transfer Details (To be filled post-approval)*

- **Mode of Transfer:** _____
- **Date of Transfer:** _____
- **Dataset Description:** _____
- **Data Format:** _____
- **Data Size:** _____
- **Transferred to (Name, Designation, Email):** _____
- **Transferred by (Name, Designation, Email):** _____
- **Transferor Signature:** _____

[i] This annexure is applicable only to the item no. 2.1.1 and 2.1.2 of the SoP. The items with * are mandatory.