POLICY ON DATA GOVERNANCE AND DATA SECURITY

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

COMPTROLLER AND AUDITOR GENERAL OF INDIA

उप महालेखाकार
(ले. एवं बी.एल.सी.) सचिवालय
DAG (A/cs & VLC) Secttt.
डायरी संख्या/Dy. No. 304
दिनांक/Date 24/10/24

Preface

Information Technology is a key driver of efficient and effective delivery of public goods and services. There has been a significant increase in the scope and volume of data being maintained in public sector information systems, including sensitive and personally identifiable information related to citizens. This data may include details on family members, medical history, income level, bank accounts, marital status etc. Protection of the privacy of the citizens and maintenance of confidentiality and integrity of such data is vital.

In this context, it is necessary that a robust framework for data governance and security be adopted by all Government entities which act as custodians of such sensitive data. As a high performing Supreme Audit Institution, we not only have to ensure that such data related to our own Officers and officials is protected with adequate safeguards, but also exercise due diligence in fulfilling our fiduciary responsibility, since we are mandated to access and analyse the data maintained by our audited entities.

This Policy on Data Governance and Data Security is an attempt to define the broad contours of how we intend to achieve the above objectives. The Policy has elements such as incorporation of the principles of privacy and security into the design of Departmental applications, creation of an institutional framework for clarity on roles and responsibilities of key personnel, classification of and security for the data that resides in our custody and guidelines for the collection and sharing of personally identifiable information.

Data Governance and Security is a rapidly evolving subject matter, with both use cases for more granular analysis as well as threats to information security emerging at unprecedented pace. We need to be cognizant of both these aspects and function as both an agile and trustworthy institution.

I am sure that the Officers and officials of the Department would find this Policy useful in guiding their actions towards enhancing the quality of public accounting and auditing, as well as in fulfilling their roles as guardians of citizens' privacy.

Girish Chandra Murmu
Comptroller and Auditor General of India
August 2024

Foreword

The Digital Personal Data Protection Act was passed by the Parliament of India in August 2023, with the objective of creating a legal framework for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.

This is a progressive legislation which recognizes the rights of data principals, i.e. the citizens and individuals over the use of their personal data and prescribes the obligations of data fiduciaries in ensuring that such personal data is collected, shared and used only for legitimate end purposes.

In order to achieve the objectives of ensuring compliance with the statutory framework, providing guidance on the management of diverse types of data utilised in the Office of the CAG of India and the IA&AD and addressing the concerns of privacy of personal data of our own personnel as well as that of individuals, collected during the course of work, this Policy on Data Governance and Data Security has been formulated.

The Policy prescribes a mechanism for oversight and monitoring of our personnel who have been entrusted with the tasks of collection, storage analysis and dissemination of personal data. The two crucial aspects which are intended to be addressed are the protection of privacy of individual citizens and employees, and the security of data in our custody. With these in mind, the Policy has provisions for specific actions and controls such as regulating access to the personal data stored in our Offices, anonymization of sensitive data fields during our audit assignments and during the upgrade of our accounting and entitlement applications, and adoption of policies for the use of portable devices and data retention.

It is envisaged that this Policy will be implemented through notification of Standard Operating Procedures for such specific actions, in due course. I am confident that all our Departmental Offices will make efforts to foster a culture of data protection and information security and internalize the responsibilities entrusted to them.

S Ramann
Chief Technology Officer,
Office of the CAG of India.
August 2024

Table of Contents

1. Preamble

1.1 Unprecedented spread of digital governance in the functions and activities of the Government of India, States and Union Territories, have changed the ways auditing, accounting and service-delivery roles are played by the Indian Audit and Accounts Department (IA&AD). Besides, IA&AD has a robust built-in digital infrastructure for auditing, accounting, entitlement functions and personnel management to deliver on the statutory roles of the Comptroller & Auditor General (C&AG) of India.

1.2 With its own applications for accounting (VLC), entitlements (SAI pension, GPF, GE applications), audit (OIOS), Finance/HR (iBEMS, SAI Training) and email (NIC), IA&AD has been generating a plethora of data. IA&AD is also part of the Government of India's larger digital architecture (e-Office, SPARROW, PFMS etc.). All these applications include personal, sensitive as well as confidential data.

1.3 Growth of Big Data analytics and Artificial Intelligence (AI) in providing hitherto unseen level of analytical capability opened arenas for innovation in functions of the Department. To accept the opportunities offered by this digital transformation and to address various dimensions relating to generation and management of data, a 'Policy on Data Governance and Data Security' is of paramount importance. It is with this background; this policy document has been prepared.

1.4 This policy on Data Governance and Data Security is issued by the Comptroller and Auditor General of India in exercise of powers conferred as per Regulation 169 of Regulations on Audit and Accounts 2020.

This policy would apply to all the data generated, acquired, and managed by the IA&AD.

2. Definitions

2.1 AI Curation Unit (earlier known as Data Management Unit) is an organizational unit in a Ministry/ Department which shall ensure dedicated capacity for managing, accessing, and using non-personal data within that Ministry/ Department.

2.2 Chief Data Protection Officer (CDPO) is an officer at the level of Director General/ Principal Director posted at the office of C&AG of India, who would supervise the functioning of the Data Protection Officers (DPOs), redress grievances of the people/entities relating to data protection/sharing and carry out periodic assessments of the data governance, privacy, and security aspects in the IA&AD.

2.3 Chief Information Security Officer (CISO) is an officer at DG/PD level posted in IS wing at the office of C&AG of India, who would supervise the overall security landscape of the organisation and defining security standards, implementing latest security solutions and technologies. His role over and above this will also follow MEITY defined roles, responsibilities and reporting of CISO.

2.4 Data, as defined in the DPDP Act, 2023, means 'a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means'.

Data include transactions, records, books, accounts, papers etc to comprehensively address whichever form data, information and documents are maintained by the auditable entity or within the IA&AD or collected through primary survey like a beneficiary survey during the field audit, an audio/video file obtained during field verification, and whether stored in a computer system or moved through any analog, printed or digital media.

2.5 **Data Principal** means the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child. For a person with disability, Data Principal includes her/his lawful guardian, acting on her/his behalf (DPDP Act, 2023).

2.6 **Data Processor** means 'any person who processes personal data on behalf of a Data Fiduciary' (DPDP Act 2023).

2.7 **Data Protection Officer** (DPO) means an Officer appointed for the purpose of implementing this policy in the IA&AD, with responsibilities as defined in the DPDP Act 2023.

2.8 **Data Owner**: Data owner is a designated authority, who shall have full rights and controls over data.

2.9 **Fiduciary Relationship** means 'a relationship of trust which may also be between a person and a juristic person such as Government, university or a bank' and fiduciaries can include public servants in relation to the Government[1]. Data Fiduciary is the 'person who alone or in conjunction with other person determines the purpose and means of processing of personal data' (DPDP Act, 2023).

[1] Ministry of Statistics and Programme Implementation. FAQs related to RTI Matters. Accessed on June 16th, 2023, from https://www.mospi.gov.in/faq-related-rti-matters

2.10 **Geo-Spatial Data** means 'all data which is geographically referenced' (NDSAP, 2012), having latitudinal, longitudinal, and altitudinal information helping locate an object on the globe.

2.11 **Information** means 'data, message, text, images, sound, voice, codes, computer programmes, software and data bases or microfilm or computer-generated micro fiche' (IT Act, 2000). Regulation of Audit & Accounts, 2020 defines information as 'any material in any form, including records, transactions, documents, memos, e-mails, opinions, advice, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data or other material held in any electronic form and information relating to any private body which can be accessed by a public authority under any law for the time being in force'.

2.12 **Negative List** means 'Non-sharable data as declared' by the IA&AD offices from time-to time. These data are not to be shared with any entity without the express permission from the CDPO.

2.13 **Personal Data** means 'any data about an individual who is identifiable by or in relation to such data' (DPDP Act 2023); and 'any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person' (IT Rules, 2011).

2.14 **Restricted Data** means 'data which are accessible only through a prescribed process of registration and authorization' (NDSAP, 2012), by IA&AD.

2.15 **Shareable Data** means 'those data not covered under the scope of negative list and non-sensitive in nature' (NDSAP, 2012).

2.16 **Sensitive Personal Information** (SPI) means 'personal data or information which consists of information relating to password; financial information such as Bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; Biometric information', etc. (IT Rules, 2011). However, if such information is freely available in the public domain, such information may not be considered as SPI.

3. Objectives

The broad objectives of the policy on data governance and data security are as mentioned below.

1. To implement a data governance, security and privacy policy structure in the IA&AD, aligned with the statutory framework of the Government of India, such as the IT Act 2000 and subsequent amendments, IT (RSPP&SPDI) Rules 2011, NDSAP 2012 and DPDP Act 2023 and any other Act as and when notified by Government of India.
2. To provide framework for management of diverse types of data utilised in the IA&AD and ensure its security.
3. To address the concerns of privacy of individuals, data held in fiduciary capacity and third-party data residing with IA&AD and develop a guidance framework for their access, usage and management.

4. Data Governance and Privacy Policy Structure:

4.1 Data as an Asset

As per IndEA 2.0 framework, Data is an asset. Data systems are to be designed in a manner that creates, supports, maintains, and enhances value to the enterprise specifically, and to the ecosystem in general.

4.2 Standards and Design

Any hardware, software, and application systems procured or developed or designed in the IA&AD should be set-up and modelled in a way that it facilitates the use of data as an asset in an efficient, economical and responsible manner. It would include:

1. **Standards**: Data generated from the various systems within IA&AD should follow uniform codes, format, designations, master data, Office names etc. as much as possible. Any new application should consider the available standardised formats of existing applications to maintain consistency and uniformity in design.
2. **Privacy by design**: All the IT systems should have appropriate architecture in place to enforce privacy principles. Protection of data privacy shall be embedded in the system design so that concerns for data privacy is already addressed at the design stage, and not included as an after-thought. For the existing systems, a review will be carried out by owners with help of expert(s) to see the possibility of including privacy related features, if needed.
3. **Security and Transparency by design**: All the systems should ensure data confidentiality, non-repudiation, integrity and availability while aiding transparency.

4. Promote establishment of Data Exchange and interoperability with stakeholders' systems following industry standards.

4.3 Institutional Framework for Data Governance

Data Owners

There shall be designated Data Owners for various categories of data maintained in IA&AD.

a. For individual field offices, respective Heads of Departments (HoDs) shall be the Data Owner. for CAG's Headquarters office, respective heads of functional wings (Deputy C&AG/ Additional Deputy C&AG) shall be the Data Owner for data owned within the functional wing and data residing in applications owned by the functional wings. CTO shall be the Data Owner for all other applications of IA&AD.

b. Role of Data Owner shall be following:

   i. Data owners are responsible for ensuring adequate security measures to protect the data they own. This includes setting up encryption of sensitive data both in transit and at rest, specification of encryption standards and procedures for encryption key management, access controls, and other security protocols to maintain data security in consultation with CTO Wing.

   ii. Data owners have the authority to make decisions about data access, usage, and retention within their jurisdiction. They control who can access the data and for what purpose.

   iii. Data owners shall define data retention and disposal policies within their jurisdiction, ensuring data is retained appropriately and securely disposed of when necessary.

c. Data owners have the responsibility to ensure data within their jurisdiction complies with relevant government regulations and standards. They may define procedures for compliance.

Chief Data protection Officer and Data Protection Officer

d. Within the Information Systems (IS) Wing, a post of Chief Data Protection Officer (CDPO) shall be created/ designated, who shall act as Nodal Officer for data governance in the IA&AD and as the Chief Information Security Officer (CISO) for the Department, as per the Guidelines issued by the Indian Computer Emergency Response Team (CERT-IN)

under the provisions of Section 70B of the IT Act. Director General/ Principal Director (IS) would be the designated CDPO and CISO.

e. Data owners within the headquarters office shall nominate a Data Protection Officer (DPO) within their wing responsible for the data within their jurisdiction.

f. The HODs in field offices will nominate a Data Protection Officer (DPO), who shall be responsible for management of data in each of the Field Offices. Data Protection Officer may be chosen at the level of Group Officer or Sr. AO (where there is no group officer post in the office).

g. DPOs shall have the following functions:

   i. review requisitions for accessing data from the Auditee and Government Departments and agencies, where the dataset involved is of high volume and electronic in nature. Where existence of such data is explored during the field audit-execution stage, the Field Audit Parties (FAPs)/Treasury Inspection Parties (TIPs) etc. shall make fresh/additional requisitions for such data and receive the same from the auditee unit. DPOs shall be informed regarding any such fresh/additional requisitions.

   ii. receive data from the field parties/teams on completion of their audit assignment, from all the portable devices, including mobile phones.

   iii. ensure management and protection of data, as provided in this policy.

   iv. facilitate capacity building of the field parties/teams and officials in the Field Offices.

   v. prepare/update list of Data, held within its jurisdiction.

   vi. redress grievances of the public/auditees relating to any data related issues and respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of the DPDP Act 2023.

   vii. carry out periodic assessments of the data governance, privacy, and security aspects in the respective jurisdiction.

   viii. respond to any emergency related to data privacy and/or security breach issues under intimation to the HoDs immediately on each occurrence and bring to the knowledge of the CDPO.

   ix. Perform any other functions, as prescribed within IA&AD.

h. CDPO shall have the following functions:

i. supervise the functioning of the DPOs in the Field Offices.

ii. handle grievances of people/ auditees, received at the C&AG headquarters.

iii. supervise the functioning of an Artificial Intelligence (AI) Curation Unit at HQ Office, which shall be established to ensure dedicated capacity for managing, accessing, and using non-personal data within the IA&AD.

iv. respond to any emergency related to data privacy and/ or security breach issues and coordinate with CERT-IN in his capacity as the CISO for IA&AD, as needed.

v. carry out periodic assessments of the data governance, privacy, and security aspects in the IA&AD and any revisions required in this policy with the approval of the CTO.

Role of CTO

i. CTO shall give directions to the HoDs, CDPO and DPOs over the data access rules and occasionally review existing controls for improvement of data protection measures. HoDs in the Field Offices shall perform similar roles in their respective offices. The CTO shall also identify sharable datasets that have the potential of enabling research and innovation and ensure their access through the IndiaAI Datasets Platform maintained by the Ministry of Electronics and IT, Government of India.

Interaction with external agencies regarding data

10. External agencies/ experts/ consultants are also consulted for providing technical inputs for Audit or Accounting/ Entitlement functions. Confidentiality Agreement, as currently signed shall include provisions relating to data privacy. Further, efforts may be put to hand over only anonymised data to such experts, while such data is transferred outside the IA&AD network. Use of such data by the external agencies/experts/consultants shall be restricted in the Confidentiality Agreement on the following lines:

"The recipient acknowledges and confirms that all data and information provided in relation to the agreement, on or after the date of this Agreement, shall be treated as confidential and shall not be used, disclosed, transferred, sold, assigned, traded, published, or otherwise disclosed by the Recipient for any purpose other than the purpose specifically agreed under this Agreement."

4.4 Negative List

A Negative List (NL) of the data and information, which cannot be shared to public under any circumstances, is to be prepared by the CDPO in consultation with other stakeholders in IA&AD. Preparation of this list shall also consider the provisions of the Right to Information (RTI) Act 2005 and subsequent amendments. Items in this list can be added or excluded based on the request(s) received from Field Offices, by the CDPO, in consultation with the SMU. Sharing of such data by Field Offices to any other offices in the IA&AD or Government organisations outside the Department would require authorisation from the CDPO.

The Negative List shall consist of three items, and shall be periodically reviewed and updated-

i. Information related to defence, national security and strategic importance for the nation.
ii. Work-in-progress for C&AG's audit products.
iii. Personally Identifiable Information (in unmasked form).

4.5 Preparation of List of Personal Data and Sensitive Personal Information and Anonymization

i. Personal Data and Sensitive Personal Information (SPI) ,received from the auditee organisations, held in each office/functional wing will be listed out by the DPO for the purpose of anonymisation so that seamless functioning/ auditing is done without having risk of disclosure of sensitive information. Preparation of this list shall also consider the provisions of the Right to Information (RTI) Act 2005 and subsequent amendments. Portion of data that can be shared to an applicant under the RTI Act, may be spelt out in the list. DPOs will send the list to the CDPO for approval.
ii. DPOs should ensure that to enhance interoperability and use the benefits of AI-driven data analysis, Field Offices may include a line in their audit intimation or communique to the auditee entities that data received during a particular auditing process could be used for other audits, which may not directly relate to the transactions of that auditee entity.
iii. Methods of anonymization, tools, techniques, and software applications to be used in the IA&AD are to be prescribed by the CPDO.
iv. The CDPO, in consultation with the Knowledge and Capacity Building Wing, would facilitate capacity building of the DPOs, regarding methods of anonymization and usage of selected tools/techniques/software applications.

v. A similar list shall be prepared by DPOs for protection of Personal Data and Sensitive Personal Information of employees in each office of IA&AD. The DPO in each office shall ensure that no unauthorised access to such personal and sensitive data takes place. CDPO shall maintain a centralised catalogue of all data of the different classifications.

4.6 Data Sharing Requests in Audit Offices

i. The data provided by auditee organisations, in electronic form to audit department would be submitted to the DPO who shall anonymise the SPI and provide the anonymised data to the functional wing/FAPs for analysis. Where such anonymisation at the level of DPO is not feasible, s/he shall, at the earliest, guide the head of the FAPs to perform the anonymisation before analysing the data. Where the Government Departments or Agencies provide data dump without any segregation, the DPO would receive such data, first identify the non-essential personal data in consultation with the audit team and take approval of the HoD before handing over the anonymised data to the Audit teams for analysis. The safe keeping of the database and key connecting the main data with the anonymised data would be the responsibility of the DPO.

ii. All requests for data sharing and exchanges between or among the different Field Audit Offices, would have to be approved by the concerned Data Owner, in consultation with the CDPO. On approval for such data sharing requests, the DPO shall ensure that only anonymised data is shared and SPIs are not shared among the different offices. Exceptions to this principle, may be made by the CDPO on case-to-case basis.

4.7 Collection of Data through Field Surveys, Beneficiary/Stakeholder Interviews and Joint Physical Verifications

i. Collection of primary data for verification of ground-level truth is an established practice in the IA&AD. Often, collections of data through field survey, beneficiary (data principal) interviews and Joint Physical Verifications (JPVs) involve gathering of personal and sensitive information from the field. Therefore, while preparing questionnaire or documents involving collection of sensitive personal information a consent for participation in such survey may be taken from the beneficiary. The participant shall retain the right to manage, review or withdraw consent, in accordance with the provisions of the DPDP Act, 2023. Such survey shall also give assurance to the survey participant that such surveys would only be used for the purpose of this audit or subsequent audit analysis and

the audit report would not contain any personally identifiable information and only aggregate result would be presented. A template for taking consent before such surveys is given below:

Template Questionnaire (may be translated to local language)
This survey is being conducted as part of the Audit of ....., with the main objective being.....
Responses collected through his survey would only be used for the purpose of the Audit. Result of the survey would be published in an aggregated form and no personally identifiable information would be published. The participant shall retain the right to manage, review or withdraw consent in accordance with the provisions of the DPDP Act 2023. The details of the Data Protection Officer for this purpose are listed overleaf.
I understand the purpose of the survey and give my informed consent to participate in this survey. *Signature of the Participant (The signature may be on physical survey form or in electronic format, when collected through OIOS toolkit. It may also be a thumb impression, where such beneficiary cannot sign the survey form. In cases where required, the field team may read out the questionnaire to the beneficiary and obtain signature/thumb impression on the survey questionnaire).*

ii. When such surveys are floated on the website of the office or in electronic form for people to respond to such questionnaire, there shall be an exclusive field to show consent of the participant with the given statement ('I understand the purpose of the survey and give my informed consent to participate in this survey'), which would allow the participant to answer questions in the survey.

iii. While collection of personal information, identity documents, photographs act as important key documentary evidence (KD) to establish Audit findings, such data shall be protected from public disclosure and DPO in the Field Offices shall ensure protection of such data. Photograph of survey participants shall not be printed in the Inspection or Audit Report, with their faces/identity visible. Primary collection of data/information from a Minor (Participants of less than 18 years of age) and from specially-abled persons (Divyang) shall not be done unless a consent is obtained from the legal guardian of the Minor/ specially-abled persons (Divyang).

4.8 Data Sharing Requests in Accounts & Entitlement Offices

Accounts and Entitlement (A&E) Offices in each State receive high volume of electronic data or generate high volume data relating to State Government employees, pensioners, GPF subscribers which contain sensitive personal (medical details, family details etc.) and financial (bank details, identification details etc.) information, which are required to be supervised by the DPO to avoid unauthorised access. DPO shall anonymise such data and establish protocol when such data is handled by any outsourced agency or personnel, on the lines of guidelines provided in section 4.3 above. Provisions under sections 4.6 and 4.7 above are also be followed, to the extent they are applicable in the A&E Offices.

5. Generation and Sources of Data in the IA&AD

1. Sources of Data utilised in the IA&AD are quite diversified. While some data are generated in IA&AD during the process of auditing, accounting, and personnel management functions; large quantum of data is also collected by the Field Offices in the Department for performing their statutory roles. These sources can be broadly categorized as follows:

a) Data Generated Internally and through Primary Surveys:

- Data generated within the department includes file noting, official correspondences, and human resources' data.
- Data generated in applications like e-Office, e-HRMS, SPARROW, KMS, iBEMS, and the website of the C&AG of India are utilized to process and manage this data.
- Data acquired during Beneficiary/stakeholders' surveys and physical verifications.

b) Data Obtained from Other Entities by the Field Offices:

- Field Audit and A&E Offices within the department acquire a significant amount of data to perform their statutory roles.
- Further, applications like One IA&AD One System (OIOS), Voucher Level Computerization, and others process and generate additional information during auditing and accounting activities.

A large quantum of data acquired by the IA&AD is held in in Fiduciary capacity.

2. National Data Sharing and Accessibility Policy (NDSAP), 2012 requires all data in a department to be classified as **shareable and non-sharable data**. Non-sharable data shall be put under a "negative list", whereas shareable data shall be made available through either open or registered/restricted access. Data owners through DPOs would prepare a list of shareable and non-shareable data under their ownership and get the approval of CDPO.
3. CTO may notify the set of identified datasets which, after suitable anonymization, may be shared for access through the IndiaAI Datasets Platform maintained by the Ministry of Electronics and IT, under open/ registered/ restricted access terms.
4. While uploading the identified datasets on the IndiaAI Datasets Platform, DPOs must ensure anonymization of sensitive information.

6. Data security

Data, as an asset, also requires to be secured through physical and logical access control, regular back-up and restoration when required. Offices shall adhere to the following guidelines:

i. All Information systems designed, developed, and acquired by IA&AD must comply with Information security architecture, as prescribed by the Government of India, such as the IT Act 2000 and subsequent amendments, IT (RSPP&SPDI) Rules 2011, NDSAP 2012, DPDP Act 2023 etc. The systems shall also comply with the requirements of ISO/IEC/IS 27001:2022. CTO Wing shall provide updates regarding requirements under any required Act/Rules/Guidelines, through issues of periodic directions.

ii. Application security testing shall be carried out for all applications.

iii. Periodic audits may be included to assess compliance with the data security policy and identify any vulnerabilities or gaps in security controls. Risk assessments to evaluate potential threats and their impact shall be included in such audits.

iv. DPOs shall ensure accuracy and completeness of data, while making plans for data protection and build reasonable safeguards to prevent data breach. DPOs shall put in place mechanisms which would not allow any unauthorised access to data, once they have been generated in the IA&AD systems or obtained from other entities or primary surveys, so that manipulation of data or intervention through unauthorised access, at subsequent stages, is ruled out.

v. A login-based access system may be implemented to monitor usage of data by authorised user in each office in case the data is residing in a server.

vi. Each office shall also keep a list of portable devices, including laptops, removable media like Hard Disk Drives, Solid State Drives, Flash Drives etc., issued to the FAPs/TIPs. Each Field Offices shall issue instructions to the FAPs to transfer all data, received during the field audit, including in personal devices like mobile phones, from the portable devices to a dedicated systems/network in office after the end of an audit assignment. The timeline for such data transfer may be fixed keeping in mind the frequency of visit of Field Audit Parties to the Field Office of the IA&AD.

vii. Storage of data in individual storage devices and computer system is discouraged. Data should be purged from the storage devices after it is restored/backed up in the non-portable system at Head offices or OIOS or other internal applications in the IA&AD. DPOs are responsible to ensure this.

viii. Portable devices, issued by the Field Offices to the FAPs/TIPs etc. shall be encrypted or password protected.

ix. Data received from the auditee entities shall be kept password-protected in the portable devices, so that unauthorised use of such data can be avoided. Such data shall not be shared/transferred through personal emails (Gmail, Hotmail etc.) by the Field Parties.

x. CDPO and DPOs shall ensure that data access is governed by need of the department. Any individual, by default, shall not have direct access to any data (whether generated in IA&AD or accessed from audited entity/primary survey), since access to data will be either controlled through login-based access for devices in the IA&AD network and password-protection (both device and data file, as mentioned above) for portable devices.

xi. Any Information system used in IA&AD, must facilitate implementation of access policy. Legacy applications must be upgraded for implementing access policy in phased manner.

xii. All data owners shall specify the lifespan of data, which shall not be less than the retention period specified by the relevant law(s) pertaining to the data, as well as GFR and Audit Manuals.

xiii. The data backup of all the electronic data shall be maintained within IA&AD or government or government empanelled Cloud Service Providers (CSPs). Frequency of data backup shall be decided by the data owners.

xiv. The policy on data governance and security would be reviewed annually or as decided by CTO.

Abbreviations

AI	Artificial Intelligence
C&AG	Comptroller & Auditor General (C&AG) of India
CDPO	Chief Data Protection Officer
CERT-IN	Indian Computer Emergency Response Team
CISO	Chief Information Security Officer
DPDP Act 2023	Digital Personal Data Protection Act, 2023
DPO	Data Protection Officer
FAPs	Field Audit Parties
FOs	Field Offices (Audit/A&E)
GE	Gazetted Entitlement
GPF	General Provident Fund
IA&AD	Indian Audit and Accounts Department
iBEMS	Integrated Budget and Expenditure Monitoring System
IT (RSPP&SPDI) Rules 2011	Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
IT Act 2000	Information Technology Act 2000
NDSAP 2012	National Data Sharing and Accessibility Policy 2012
NL	Negative List
OIOS	One IA&AD One System
SAI-Pension	System Automation Initiative- Pension
SPARROW	Smart Performance Appraisal Report Recording Online Window
SPI	Sensitive Personal Information
TIPs	Treasury Inspection Parties
VLC	Voucher Level Computerisation

Comptroller and
Auditor General of India
http://www.cag.gov.in