Draft

HARYANA STATE DATA EXCHANGE AND GOVERNANCE POLICY, 2026

A unified policy for secure data exchange, sharing, governance, retention, and protection

Enabling Secure, Citizen-Centric & Innovation-Driven Governance

Version 1.0

Confidential – For Official Use Only

Date - June, 2026

Draft Policy Prepared by:

Secretariat for Information Technology

Citizen Resources Information Department (CRID)

Government of Haryana

Table of Contents

1. Preamble and Policy Context

WHEREAS the Government of Haryana recognises data as a strategic sovereign resource and a foundational driver of evidence-based governance, inclusive public service delivery, and sustainable socio-economic transformation;

AND WHEREAS it is necessary to establish a unified, enforceable framework for the secure collection, storage, classification, exchange, sharing, retention, archival, protection, and ethical utilisation of all data generated, held, or processed by entities of the Government of Haryana;

AND WHEREAS it is expedient to issue this Policy as a binding instrument setting out enforceable provisions, decision rights, and obligations applicable across all State entities, in line with the Digital Personal Data Protection Act, 2023 and the National Data Governance Framework Policy of the Ministry of Electronics and Information Technology (MeitY);

NOW, THEREFORE, the Secretariat for Information Technology, Citizen Resources Information Department (CRID), Government of Haryana, hereby notifies the Haryana State Data Exchange and Governance Policy, 2026 ("this Policy"), as set out below.

2. Short Title, Extent, Application and Commencement

2.1 This Policy may be called the Haryana State Data Exchange and Governance Policy, 2026.

2.2 It extends to all territories under the jurisdiction of the Government of Haryana, including data hosted within the State as well as data processed by third parties in India or abroad on behalf of the State.

2.3 It shall come into force on and from the date of its notification in the Official Gazette and shall remain in force until superseded, amended, or withdrawn.

2.4 Application

This Policy shall apply to:

- All Departments, Boards, Corporations, Authorities, Missions, Societies, Entities and Agencies of the Government of Haryana;
- All Urban Local Bodies (ULBs), Municipal Corporations, Panchayati Raj Institutions (PRIs), and local self-government bodies;
- All State Public Sector Undertakings, State-run Institutions, and Autonomous Bodies under the Government of Haryana;
- All District Administrations, Sub-Divisional Offices, and Tehsil offices generating or processing government data;
- Private sector entities and technology partners acting as Data Processors under contract; and academic, research, start-up, and civil-society entities authorised to access State data.

2.5 Overriding Effect and Legal Conformity

2.5.1 This Policy operates in consonance with the Digital Personal Data Protection Act, 2023; the Information Technology Act, 2000 (as amended); the National Data Sharing and Accessibility

Policy, 2012; the Right to Information Act, 2005; the Public Records Act, 1993; and all other applicable laws.

2.5.2 In the event of any conflict between this Policy and a central enactment, the central law shall prevail. In the event of any inconsistency between this Policy and a departmental instruction, this Policy shall prevail to the extent of the inconsistency.

3. Definitions

In this Policy, unless the context otherwise requires, the following expressions shall bear the meanings assigned to them below. Terms not defined herein shall carry the meaning assigned in the applicable law.

Term	Meaning
Personal Data	Any data relating to an identified or identifiable natural person, as defined under the DPDP Act, 2023.
Sensitive Personal Data	Personal data including financial details, health records, biometric identifiers, caste, religion, or any category classified as sensitive under applicable law.
Non-Personal Data	Data that does not identify or make identifiable a natural person, including aggregated, anonymised, or community datasets.
Data Principal	The individual to whom personal data relates; the citizen as the ultimate owner of their personal information.
Data Fiduciary	Any government department, agency, or entity that determines the purpose and means of processing personal or non-personal data.
Data Processor	Any entity processing data on behalf of a Data Fiduciary, including private vendors, contractors, or technology partners.
SCDO	The State Chief Data Officer heading the day-to-day operations of the State Data Authority.
HSDL	The Haryana State Data Lake — the centralised, federated, multi-domain repository established under this Policy.
HDeX	The Haryana Data Exchange Platform — the governed, consent-driven platform for secure data sharing established under this Policy.
HPPA	The Haryana Parivar Pehchan Authority, the State's authoritative family and citizen identity registry (Family ID / PPP).
Data Product	A catalogued, metadata-described, access-controlled dataset or service published on HDeX for consumption by an authorised party.
Consent Artefact	A machine-readable, auditable record evidencing a Data Principal's grant, modification, or revocation of consent.
Golden Record	The single, authoritative, reconciled version of a data entity (citizen, land parcel, asset) derived from multiple source systems.
Virtual Asset	Any digital representation of value that can be digitally traded, transferred, or used for payment.

Term	Meaning
DRRS	The Departmental Record Retention Schedule maintained by each Data Fiduciary under Chapter 13 of this Policy.

4. Policy Objectives

This Policy is directed towards the following objectives:

4.1 To establish enforceable governance, ownership, and accountability for all data assets held by State entities.

4.2 To protect the privacy and rights of every citizen in full compliance with the DPDP Act, 2023.

4.3 To standardise data quality, metadata, classification, and interoperability across all government entities.

4.4 To operationalise the Haryana State Data Lake (HSDL) and the Haryana Data Exchange Platform (HDeX) for cross-domain analytics, consent-driven sharing, and innovation.

4.5 To mandate citizen consent management as the lawful basis for processing personal data, save for permitted exceptions.

4.6 To publish anonymised, non-personal Open Datasets to foster research, entrepreneurship, and civic engagement.

4.7 To embed security, auditability, and continuous improvement into the entire data lifecycle.

5. Guiding Principles

All decisions, processes, and institutions established under this Policy shall be governed by, and remain subject to, the following binding principles:

- **Citizen Sovereignty and Centricity —** Citizens are the ultimate principals of their personal data; their rights, dignity, and welfare are placed at the core.
- **Accountability and Transparency —** Roles, responsibilities, and decision rights are clearly assigned, documented, auditable, and explainable.
- **Data Integrity and Quality —** Data shall be accurate, complete, consistent, timely, and reliable, in standardised formats and metadata.
- **Privacy by Design and Security —** Protection is embedded into every lifecycle stage, supported by zero-trust architecture.
- **Data Minimisation and Purpose Limitation —** Only the minimum data necessary for a clearly defined, lawful purpose shall be collected, and personal data shall be processed only for that purpose.
- **Interoperability and Open Standards —** Open standards, APIs, and protocols enable seamless, secure exchange of data across departments, districts, agencies, and central government systems.

- **Ethical and Non-Discriminatory Use —** Use of data for unlawful profiling, surveillance, or any purpose contrary to fundamental rights is prohibited.
- **Innovation and Open Data —** Non-personal and anonymised datasets are made available to spur research and economic growth.
- **Federated Architecture and Data Sovereignty —** Sensitive and critical data is stored within the State's sovereign infrastructure.
- **Legal and Regulatory Compliance —** All activities comply with the DPDP Act 2023, IT Act 2000, NDSAP 2012, and applicable law.
- **Capacity Building and Digital Literacy —** Sustained investment in human capital ensures effective and evolving implementation.

6. Institutional Mechanism and Decision Rights

A three-tier institutional architecture shall govern data across all levels of the State, with the responsibilities set out below:

6.1 Haryana State Data Governance Council (HSDGC) — Governing Body

The Council shall be chaired by the Chief Secretary, Haryana, with the Chief Information Security Officer (CISO), the Chief Executive Officer, Haryana Parivar Pehchan Authority (HPPA), Head SeMT and the Administrative Secretaries of key departments, or their duly nominated representatives, as Members. The Head of Department, Secretariat for Information Technology (SIT), Citizen Resources Information Department (CRID), at the level of Secretary/Special Secretary/Additional Secretary, shall serve as Convenor-cum-Member Secretary of the Council. Other members may be nominated from relevant organisations, as required.

The Council shall have the following key roles & responsibilities:

- Provide strategic oversight and policy direction, and approve all amendments to this Policy;
- Ensure alignment with the Data Protection Board of India and central mandates;
- Review annual compliance and performance reports and integration-health metrics.

6.2 State Data Authority (SDA)

The SDA shall be the nodal implementing authority, chaired by the Administrative Secretary, Citizen Resources Information Department (CRID), with the Head of Department, Secretariat for Information Technology (SIT), CRID, the Chief Executive Officer, Haryana Parivar Pehchan Authority (HPPA), Head SeMT, Chief Information Security Officer (CISO), HOD from concerned departments, or their duly nominated representatives, as Members. The State Chief Data Officer (SDCO), Secretariat for Information Technology (SIT), Citizen Resources Information Department (CRID), shall serve as Convenor-cum-Member Secretary of the State Data Authority. Other members may be nominated from relevant organisations, as required.

The Authority shall have the following key roles & responsibilities:

- Drive implementation of this Policy and ensure adherence by all entities;
- Develop and operate the Haryana State Data Catalogue, the HSDL, and the HDeX;

- Monitor compliance, publish Annual State Data Reports, and issue Standard Operating Procedures (SOPs);
- Report data breaches to the Data Protection Board of India;
- Serve as the nodal agency for collaboration with industry, academia, and central and other State governments.

6.3 Departmental Data Committees (DDC)

Chaired by the Head of each Department, comprising the Departmental Data Officer (DDO), Sub-Data Officers, a Data Analyst, and the nodal officer of the concerned department. Each DDC shall:

- Classify departmental datasets and maintain entries in the State Data Catalogue;
- Ensure secure collection, storage, and sharing of departmental data, and maintain audit trails;
- Report data breaches to the SCDO within four (4) hours of detection;

6.4 Supporting/Implementation Mechanisms

A Technical Support Unit (TSU) under the SDA shall provide audit tools, integration support, and advisory services.

7. Data Classification and Ownership

7.1 Every dataset shall be classified at the point of creation or acquisition into one of the classes set out below, and the classification shall be recorded in the Haryana State Data Catalogue with its applicable access protocol.

7.2 Data Owners shall periodically review and reclassify datasets based on changes in sensitivity, legal requirements, or usage. Classification disputes (if any) shall be decided by the SDA.

Class	Description	Access Mode
Open Data	Non-sensitive, freely shareable data.	Public portal, machine-readable, no restrictions.
Sharable Data	Non-sensitive data requiring authorisation.	Formal request / MoU via HDeX.
Restricted Data	Operationally sensitive, limited access.	Role-based access with approval.
Sensitive Data	Personal / critical State data under the DPDP Act.	Consent-driven, encrypted, audited.
Transactional Data	Real-time service / administrative records.	Departmental authorisation, audit trail, retention policy.
Negative List Data	Explicitly non-shareable on sovereignty, security, or privacy grounds.	Not shareable except as required by law.

8. Data Lifecycle Management and the Haryana State Data Lake (HSDL)

This Policy applies to all stages of the data lifecycle: collection, storage and classification, processing and AI/ML application, sharing and publication, security and access control, and archival, retention, and secure disposal.

8.1 Establishment of the HSDL

8.1.1 The SDA shall establish and operate the Haryana State Data Lake (HSDL) — a centralised, federated, multi-domain repository — modelled on the NHAI Data Lake 3.0 principles and adapted for State multi-sector needs.

8.1.2 The HSDL shall adopt a federated design with multi-tier storage, an API-first integration model, hosting on the Haryana State Data Centre with geographically separated disaster recovery, and conformity with MeitY cloud and data-residency guidelines.

8.2 Priority Domains

The HSDL shall integrate data streams from the following priority domains within the first two years of operation:

Domain	Primary Departments
Citizen Services (Saral, Antyodaya, beneficiary records)	IT, Revenue, Social Justice
Land & Revenue (records, mutations, registrations)	Revenue, Registration
Agriculture (crop data, farmer registries, mandi)	Agriculture, Horticulture
Health (HMIS, hospital, vaccination data)	Health & Family Welfare
Education (enrolment, results, teacher data)	School & Higher Education
Finance (budget, treasury, scheme fund flows)	Finance, Treasury
Urban Services (property tax, water, permissions)	Urban Local Bodies
Transport (vehicle, DL, traffic analytics)	Transport, Police

8.3 HSDL Integration with the Haryana Parivar Pehchan Authority (HPPA)

8.3.1 The HSDL shall establish a mandatory, secure, real-time bi-directional communication channel with the HPPA, the State's authoritative family and citizen identity registry and foundational Digital Public Infrastructure.

8.3.2 Outbound (HSDL → HPPA): The HSDL shall push enriched, verified, consolidated citizen and household data from departmental systems to maintain the currency of Family ID records.

8.3.3 Inbound (HPPA → HSDL): HPPA shall transmit authoritative Family ID records, household composition, and socio-economic classification updates in real or near-real time, feeding the HSDL Golden Record framework.

8.3.4 All exchanges shall use TLS 1.3 encrypted REST/GraphQL APIs with mutual TLS authentication, an event-driven sync layer, consent-gated flows for sensitive personal data, and immutable audit trails retained for at least seven (7) years.

8.3.5 A formal Data Sharing Agreement shall be executed between the SDA and HPPA. Any change to the HPPA schema, Family ID structure, or API specification shall be notified to the SCDO with a minimum of sixty (60) days' notice.

9. Haryana Data Exchange Platform (HDeX)

The SDA shall establish the **Haryana Data Exchange Platform (HDeX)** as a federated Digital Public Infrastructure: a governed, consent-driven, and auditable marketplace for secure data sharing among government departments, the private sector, academia, and civil society.

9.1 Design Principles

The HDeX shall embody the following design principles:

- **Data exchange as the backbone of AI adoption —** HDeX shall be positioned as the foundational layer enabling AI/ML innovation on governed, consented data.
- **Federated DPI architecture —** Departments retain ownership of their data products while the exchange provides discovery, consent validation, and controlled access.
- **Sector-by-sector rollout —** HDeX shall prioritise high-impact sectors (health, agriculture, transport, education, civil supplies) through pilot use-cases before scaling State-wide.
- **Data Product Catalogue —** A browsable directory of available datasets, each described by standardised metadata and maintained by the publishing department.
- **Consent integration —** HDeX shall validate consent status before any personal-data transaction.
- **Immutable audit trail —** Every access, query, and transaction shall be logged immutably for compliance and accountability.

9.2 Transaction Categories

Category	Scope
Government-to-Government (G2G)	Seamless departmental data sharing with authorisation controls.
Government-to-Business (G2B)	Controlled release of anonymised or shareable datasets to industry under MoU / data-licensing agreements.
Government-to-Academia (G2A)	Research data access for universities and institutions under ethical-use agreements.
Government-to-Citizen (G2C)	Access to open datasets and personal-data dashboards via citizen-facing portals.

9.3 Governance and Interoperability

9.3.1 HDeX shall be administered by the SDA. Departments shall publish Data Products and remain responsible for their accuracy and metadata completeness.

9.3.2 Consumer onboarding shall require identity verification, purpose declaration, and compliance attestation. Data-use agreements shall specify permissible purposes, retention limits, and a prohibition on derivative commercialisation.

9.3.3 HDeX shall be designed for future interoperability with national data-exchange frameworks and other State and central data platforms, using Open API 3.0 and the metadata standards adopted under this Policy.

10. Beneficiary Identification, Golden Record, and Welfare Targeting

To strengthen welfare targeting and reduce leakage across flagship schemes, this Policy mandates the following measures, anchored upon the Parivar Pehchan Patra (PPP) data foundation — which enables cross-departmental record linkage and provides a single authoritative citizen/family identifier:

10.1 The SDA shall operationalise a Golden Record / Master Data Management framework to create authoritative, reconciled master records for citizens, land parcels, and public assets, with the Family ID (PPP) as the primary unifying identifier.

10.2 A de-duplication engine shall operate at the HSDL–HPPA interface using the Family ID to resolve duplicate or conflicting citizen records across all departmental datasets.

10.3 Eligibility attributes — income, caste, land holding, disability, and government-pensioner status — shall be fetched through the Family ID without requiring fresh document submission, subject to consent and access controls.

10.4 The SDA may, on the PPP foundation, pilot a Welfare Schemes Eligibility Management capability on two or three high-leakage schemes to demonstrate measurable savings before scaling, and shall establish the governing data-sharing and consent protocols for such use.

11. Consent Management

11.1 Consent shall be the lawful basis for processing personal data within the State data ecosystem, save where exceptions apply under the DPDP Act, 2023.

11.2 The SDA shall establish and operate a Haryana Consent Management Portal, accessible via web and mobile in English, Hindi, and regional Haryanvi dialects, through which citizens may grant, review, modify, or revoke consent at any time.

11.3 Consent receipts shall be issued digitally for every consent transaction, and consent dashboards shall display active consents, usage history, and pending requests.

11.4 Withdrawal of consent shall not affect access to essential public services.

11.5 Citizen Rights

Every Data Principal shall have the rights to information, access, correction, erasure (subject to statutory retention), and grievance redressal, exercisable through the Departmental Data Committee or the SDA within defined timelines.

11.6 Exceptions to Consent

Personal data may be processed without explicit consent only in the limited cases permitted under the DPDP Act, 2023, namely: compliance with legal obligations of the State; medical emergencies and disaster response; functions of the State in the interest of sovereignty, security, or public order; and anonymised or aggregated data used for statistical, research, or public-interest purposes.

11.7 Departmental Responsibilities

Departments shall record consent before processing personal data, store consent records securely and traceably, report consent violations to the SDA within twenty-four (24) hours, and publish annual transparency reports.

12. Data Protection and Security

Security controls shall be governed by the principles of Privacy by Design, Zero Trust, Proportionality, Resilience, and Transparency.

12.1 Technical Standards

- Encryption: minimum AES-256 at rest; TLS 1.3 or higher in transit; end-to-end encryption for sensitive and transactional datasets, aligned with CERT-In guidelines.
- Access control: role-based, need-to-know models; mandatory Multi-Factor Authentication for all privileged accounts; Privileged Access Management for critical systems; periodic review and revocation of dormant accounts.
- Anonymisation: verified anonymisation before analytics or public release; pseudonymisation only in controlled research environments with re-identification controls.
- Backup and recovery: automated encrypted backups; geographically separated DR; defined RTO/RPO per data class; periodic DR testing reported to the HSDGC.

12.2 Incident Management

12.2.1 Data Analysts shall report breaches to the DDO within four (4) hours; the DDO shall escalate to the SCDO within six (6) hours; the SCDO shall report to the Data Protection Board of India and CERT-In within statutory timelines.

12.2.2 Post-incident reviews shall be mandatory within thirty (30) days, with learnings incorporated into subsequent revisions of this Policy.

12.3 Erasure and Emerging Technology Safeguards

12.3.1 Each Data Fiduciary shall operationalise the Right to Erasure in accordance with statutory retention requirements, retaining only lawfully required ancillary records (logs, metadata, audit trails). Retention periods, archival, and certified disposal.

12.3.2 AI-based processing shall incorporate fairness, transparency, auditability, and bias-detection mechanisms. Blockchain may be used for tamper-evident audit trails (e.g., land and property records). IoT, edge, and cloud deployments shall comply with device-level security and MeitY data-residency requirements.

13. Data Retention and Archival

This Chapter establishes the binding regime for the retention, archival, and secure disposal of records held by State entities, in physical and electronic form.

13.1 General Provisions

13.1.1 Each Data Fiduciary shall define data retention periods according to functional requirements and legal obligations, recorded in a Departmental Record Retention Schedule (DRRS).

13.1.2 No record shall be destroyed prior to the expiry of the retention period specified in the DRRS.

13.1.3 On expiry, data shall be archived or securely destroyed in accordance with approved protocols. Archived data may be used for research or analytics only after verified anonymisation.

13.1.4 The Head of Department / Records Officer shall ensure secure storage, correct classification, and adherence to retention rules, supported by technical controls (encryption, logging, access management) and periodic compliance audits.

13.1.5 Records classified as Category A (permanent) or otherwise required for long-term preservation shall be transferred to archival custody in accordance with State Archives procedures and this Policy. The Haryana State Digital Repository / State Data Archives Cell shall serve as the repository for official and archival electronic records.

13.2 Classification of Physical Records

Category	Meaning / Classification	Retention Requirement
Category A — Keep and Microfilm	Records of permanent value or historical importance; precious documents or those requiring frequent reference.	Permanent preservation; microfilming required.
Category B — Keep, but do not Microfilm	Permanent preservation, but not valuable enough for microfilming.	Permanent preservation (administrative importance).
Category C — Keep for specified period only	Records of secondary importance.	Retain for limited years (3 / 5 / 10) as per schedule (C-3 / C-5 / C-10).
Category C-3 / C-5 / C-10	Sub-classification defining retention duration.	Keep for 3, 5, or 10 years, respectively.

13.3 Classification of Electronic Records

Category	Meaning / Classification	Retention Requirement
Category I — Permanent	Records of historical importance.	Keep 10 years on the departmental server, then transfer to the State Data Archives Cell with a copy to the respective entity.
Category II — Secondary importance	Records useful for reference.	Keep 10 years on the server; may be upgraded to Category I if required.

13.4 Retention Schedule

Record / Data Type	Owner	Classification	Retention	Backup / DR	Final Action
Records of historical importance / precious documents	Record Section / Dept.	Category A	Permanent (keep & microfilm)	—	Permanent preservation
Permanent administrative records	Concerned Dept.	Category B	Permanent (keep)	—	Permanent preservation
Temporary office files	Concerned Division	Category C (C-3 / C-5 / C-10)	3 / 5 / 10 years	—	Destroy after expiry
Electronic records — Category I (historical)	IT / Dept.	Digital — Cat. I	10 yrs, then transfer	As per server retention	Archive
Electronic records — Category II (secondary)	IT / Dept.	Digital — Cat. II	10 yrs on server	As per server retention	Delete
ICT system logs	IT / Data Centre	Digital	180 days (rolling)	Stored in India	Delete
VPS / Cloud / VPN subscriber data	IT / Data Centre	Digital	5 years	As per CERT-In	Delete
Virtual Asset (crypto) KYC & transaction records	IT / Finance	Digital	5 years	As per CERT-In	Delete

14. Open Data

14.1 The SDA shall operate the Haryana Open Data Portal, publishing anonymised, non-personal datasets in machine-readable formats under the Dublin Core / DCAT metadata standards.

14.2 Departments shall progressively publish their non-sensitive datasets, prioritising those of high value to research, entrepreneurship, and civic engagement, in alignment with the NDSAP, 2012.

15. Vendor and Third-Party Management

Flagship State data platforms may be operated through a competent System Integrator under an operations-and-enhancements contract governed by clear service-level agreements and DPDP compliance, under the oversight of the SDA under SIT, CRID. All contracts involving State datasets shall include mandatory Data Processing Addendum provisions requiring:

- Breach notification to the State within six (6) hours of detection;
- Full indemnification of the State against penalties arising from vendor non-compliance;
- Right of the State to audit vendor systems and data-processing operations at any time;

- Prohibition on derivative commercialisation of State data without explicit SDA approval;
- Return or secure deletion of State datasets and derived artefacts upon contract termination.

16. Monitoring, Audit, and Continuous Improvement

16.1 Performance Monitoring

The SDA shall maintain a real-time compliance dashboard tracking, inter alia, the proportion of departments with classified catalogues, open datasets published, metadata-compliance rates, breach incidents, consent-adoption rates, and citizen-satisfaction scores.

16.2 Two-Tier Audit

16.2.1 Tier I — Internal Departmental Audit: All Data Fiduciaries shall conduct internal audits at least annually and submit reports to the SDA.

16.2.2 Tier II — Independent Statutory Audit: Entities designated as Significant Data Fiduciaries shall be subject to periodic independent audit by a qualified Data Auditor, reporting to the HSDGC and, where required, to the Data Protection Board of India. The HPPA integration interface shall fall within the scope of such audits, with integration-health metrics reported quarterly to the HSDGC.

16.3 Reporting and Review

- Quarterly Compliance Reports: Departmental Data Committees to the State Data Authority (SDA);
- Annual State Data Governance Report: Published by the SDA;
- Public Transparency Report: Non-sensitive audit findings published for public accountability;
- This Policy shall be reviewed comprehensively at least once every three (3) years by the SDA and Haryana State Data Governance Council (HSDGC)

17. Capacity Building and Implementation

17.1 The SDA shall issue mandatory SOPs covering classification and cataloguing, HDeX access requests, consent operations, breach notification, vendor data-processing agreements, and open-data publication.

17.2 Annual training and certification programmes shall be conducted for Data Officers, Data Analysts, and IT staff, in collaboration with premier institutions (including HIPA and MeitY-empanelled agencies), supported by a Haryana Data Governance Knowledge Repository and citizen-awareness campaigns.

17.3 The expenditure requirements may be met/provisioned under the IT Plan Budget Head/Society for IT Initiative Fund for e-Governance, as required.

18. Enforcement, Penalties, and Statutory Backing

18.1 Non-compliance with this Policy by a State entity shall be reported to the HSDGC and may attract administrative action, withdrawal of departmental data from HDeX/HSDL and other digital-access privileges, and direction for remedial compliance within a stipulated period.

18.2 Penalties arising under the DPDP Act, 2023 or other applicable law for breaches by Data Fiduciaries or Data Processors shall be borne and addressed in accordance with that law;

19. Amendment and Repeal

19.1 This Policy may be amended, supplemented, or repealed by the SDA with the approval of the HSDGC.

19.2 All amendments shall be notified and incorporated into the Haryana Data Governance Knowledge Repository, and the effective version shall be published on the official portals of the Haryana Government Gazette and DITECH.