Data Protection Policy

The Data Protection Policy of the Indian Institute of Management Indore establishes a comprehensive framework for collecting, processing, storing, and protecting personal and institutional data. It ensures legal compliance, ethical management, and robust security across all digital and physical records handled by the Institute community.

Key Core Components

1. Scope and Governance

- **Applicability:** The policy governs all students, faculty, administrative staff, research scholars, alumni, contractual workers, and third-party vendors.
- **Data Ownership:** All data generated or stored using Institute resources remains the exclusive property of IIM Indore.
- **Governance Structure:** Oversight is maintained through Data Protection policy, designated data owners, custodians and periodic audits. The policy is reviewed every two years or in response to regulatory and technological changes.

2. Core Data Protection Principles

The Institute adheres to six fundamental data principles:

- **Lawful & Transparent Processing:** Data is collected solely for legitimate academic, research, and administrative purposes, with transparency provided to data subjects.
- **Purpose & Data Minimization:** Collection is restricted only to necessary data, which cannot be used for unrelated purposes without authorization.
- **Accuracy & Storage Limitation:** Data is kept accurate, updated, and retained only as long as legal, academic, or institutional obligations require.
- **Security & Confidentiality:** Technical and organizational measures are enforced to prevent unauthorized access, loss, or misuse.

3. Data Categories & Access Control

- **Data Types:** Covered data includes student academic/placement records, employee payroll/performance metrics, research materials, campus security (CCTV/visitor logs), and IT system activity logs.
- **Access Protocols:** Access is strictly granted on a **"Need to Know"** and **"Least Privilege"** basis. Role-based access control is implemented, and user permissions are revoked immediately upon a change in role or separation from the Institute.

- **Personal data in the public domain**

  We hold certain information about faculty, staff and students in the public domain. Personal data classified as being in the 'public domain' refers to information which will be publicly available worldwide and may be disclosed to third parties without recourse to the data subject. There is certain information under the Suo Moto Disclosure under RTI Act-2005 are available on public domain.

  Our practice is to make the following items of data freely available unless individuals have objected:

- Names of members of Committee, club and offices, employee workplace email addresses and telephone numbers, student institute's email addresses, academic staff biographies and curricula vitae where supplied names and academic qualifications and support staff where appropriate.

- Any additional information relating to data subjects which they have agreed to be placed in the public domain, and which may be in automated and/or manual form.

4. Data Security, Storage & Governance

- **Infrastructure Security:** Safeguards include strong password mandates, multi-factor authentication (MFA), data encryption, firewalls, antivirus endpoint protection, and regular vulnerability assessments.

- **Storage, Backup and Cloud Protocols:** Critical institutional data is backed up regularly and tested periodically in alignment with the Institute's Disaster Recovery (DR) Plan. Third-party cloud services undergo strict security and data-ownership evaluations before deployment. Data shall not be retained longer than required unless required by legal, regulatory, academic, or archival obligations.

- **Official Communications:** Users are required to use official email accounts for institutional communications and are prohibited from sharing confidential data via personal storage or personal email.

5. Incident Management and Individual Rights

- **Data Breaches:** Any suspected data breach or cybersecurity incident must be reported immediately to the IT/security team for containment, stakeholder notification, and corrective action.

- **Privacy Rights:** Data subjects retain the right to request information about their personal data, correct inaccuracies, seek clarification on usage, or withdraw consent where legally applicable.

6. User Responsibilities

Do's & Don'ts for the IIM Indore Community

- **Do:** Protect login credentials, use official email channels, verify recipients before transferring information, and report suspicious activities immediately. On requirement basis Information to be shared with third parties with approval of the competent authorities.

- **Don't:** Share passwords, install unauthorized software, access data beyond authorized permissions, or store institutional data on personal devices without prior approval. Disclosing official/personal data to a third person inside/outside the institute without the consent of the data subject.

Review Frequency: Every 2 years