Data Security Policy

The **Digital Personal Data Protection (DPDP) Act, 2023** establishes a structured framework for data security and privacy in India.

1. Purpose

This policy outlines the measures taken to protect personal data in compliance with the **DPDP Act, 2023** and the **DPDP Rules, 2025**. It ensures secure data processing, storage, and transfer while safeguarding individuals' rights.

2. Scope

This policy applies to all employees, third-party vendors, and stakeholders handling personal data within the organization.

3. Data Collection & Processing

- Personal data shall be collected **only with explicit consent** from the data principal.
- Data processing must be **lawful, fair, and transparent**.
- Sensitive personal data requires **additional safeguards**.

4. Data Security Measures

- **Encryption:** All personal data should be encrypted during storage and transmission as far as consider feasible taking into account the nature and size of the organisation.
- **Access Control:** Role-based access should be implemented to restrict unauthorized data access.
- **Breach Notification:** Any data breach must be reported to the **Data Protection Board of India** within **72 hours**.
- **Regular Audits:** Periodic security audits should be conducted to ensure compliance.

5. Rights of Data Principals

- Individuals have the right to **access, correct, and erase** their personal data.
- They can **withdraw consent** at any time.
- Organizations must provide a **grievance redressal mechanism**.

6. Cross-Border Data Transfers

- Personal data can be transferred outside India **only to trusted jurisdictions** as per DPDP guidelines.
- Adequate safeguards must be in place to protect transferred data.

7. Compliance & Penalties

- Non-compliance with the DPDP Act may result in **financial penalties** and regulatory action.
- Employees must undergo **mandatory training** on data protection as may be arranged by the organisation from time to time.