



Himadri Speciality Chemical Ltd

CIN: L27106WB1987PLC042756

INFORMATION SECURITY & DATA MANAGEMENT POLICY MANUAL

Version	Revision/Review Date	Approved By	Date Approved
Adopted on	-	ESG Council	08.12.2023
V1	-	ESG Council	16.09.2026

1.Data Management Framework

Data Collection and Use

- All data collected must have a clear purpose, and stakeholders must be informed about how their data will be used.
- Consent must be obtained for the collection of personal data as per DPDP 2023 requirements.

Data Storage

- Data will be stored in secure, encrypted systems that comply with both national regulations and internal standards.
- Only authorized personnel will have access to sensitive data, and access will be logged and monitored.

Data Retention and Disposal

- Data will be retained as per legal and regulatory requirements.
- Upon reaching the end of its lifecycle, data will be securely deleted or anonymized to prevent unauthorized access.

Data Access and Sharing

- Access to data will be role-based and restricted according to the principle of least privilege.
- Data sharing with third parties must be governed by strict contractual agreements ensuring compliance with DPDP 2023 and internal policies.

2. Security Measures

Cybersecurity Practices

- All systems managing sensitive data will have robust security measures, including firewalls, encryption, and regular vulnerability assessments.
- Multi-factor authentication (MFA) and strong password policies will be enforced to prevent unauthorized access.

Incident Response Plan

- In the event of a data breach, the response plan will be activated, and the necessary notifications will be made as required by law.
- Post-incident audits will be conducted to assess vulnerabilities and implement improvements.

Data Anonymization and Encryption

- Sensitive personal data will be anonymized or encrypted in all data transfers to ensure privacy and security.

3. Monitoring and Reporting

- **Data Protection Audits:** Conducted annually to ensure adherence to policy standards and identify areas for improvement.
- **Key Performance Indicators (KPIs):** Monitored to assess compliance with training completion rates, incident reporting, and third-party adherence to contractual obligations.
- **Whistle-blower Protection:** Providing employees and stakeholders with secure channels to report any data-related misconduct or breaches.

4. Policy Framework Review

This framework will be reviewed every three years and updated as necessary to reflect changes in Indian laws, technological advancements, and evolving market conditions. The Sustainability (ESG) Council will oversee the review process.

By adhering to this Information Security & Data Management framework, Himadri aims to create a secure, compliant, and transparent data environment, ensuring the protection of personal and organizational data in line with India's regulatory framework and global best practices.

Dated: 16.09.2026

Sd/-
Anurag Choudhary
Chairman-cum-Managing
Director & CEO