Himadri Speciality Chemical Ltd

Information Security & Data Management Policy

Policy Version :1.0/2023	(w.e.f :10th December, 2023)

	Prepared By	Reviewed By		Approved By
Name	Mr. Vishnu Arat	Ms. Monica Saraswat	Mr. Avijit Sasmal	Mr. Anurag Choudhary
Designation	Sr. Manager– HSE & Sustainability	Company Secretary	Sr. Vice President- HSE & Sustainability	CMD & CEO
Signature				
Date	07.12.2023	07.12.2023	07.12.2023	08.12.2023

Purpose

Himadri is committed to building trusted partnerships through secure and transparent data handling practices. This policy reflects the organization's commitment to:

- Ethical data usage
- Secure and reliable data handling
- Compliance with laws and regulations

Data is critical for efficient decision-making and business processes. The aim is to ensure that our data management practices align with legal requirements, specifically the Digital Personal Data Protection Act (DPDP), 2023, and foster a security-aware culture across the organization.

Scope

This policy applies to all data activities in Himadri, including:

- **Employees**: Permanent and contract employees
- **Facilities**: All manufacturing plants, corporate offices, subsidiaries and remote work setups
- **Stakeholders**: Partners, third-party service providers, and customers

The policy covers all aspects of data handling, including collection, storage, usage, and disposal, in compliance with Indian regulations and applicable international standards.

Organization and Responsibilities

Data protection is a **shared responsibility** across all departments. While the IT department manages the technical infrastructure, every employee, partner, and third party involved with Himadri must comply with this policy. Responsibilities are structured as follows:

- **IT Department**: Manages data security infrastructure and ensures compliance with technical standards.
- **Employees**: Must follow best practices in data handling, report incidents, and participate in mandatory training.
- **Third-party Vendors**: Will be required to adhere to contractual obligations regarding data protection.

Our Beliefs

- **Privacy is a Fundamental Right**: Adhering to India's legal framework and respecting individuals' right to data privacy.
- **Security is a Shared Responsibility**: Ensuring everyone in the organization participates in safeguarding data.
- **Ethical Data Use**: Promoting transparency and ethical practices in handling personal and operational data.
- **Data Integrity and Accuracy**: Maintaining high standards of data quality and avoiding the manipulation of data.
- **Compliance with Laws**: Strict adherence to the Digital Personal Data Protection Act, 2023, and other relevant regulations.

Our Aims

- **Safeguard Sensitive Data**: Protect personal, financial, and operational data from unauthorized access.
- **Ensure Compliance**: Maintain compliance with Indian and global data regulations.
- **Mitigate Risks**: Proactively manage and mitigate risks related to data security breaches.
- **Protect Intellectual Property**: Safeguard proprietary information and company assets.
- **Foster Trust and Accountability**: Build stakeholder trust through responsible data practices.

Our Commitments

- **ISO 27001:2022 Certification**: Implementing an information security management system across all operations by 2026.
- **Employee Training**: Achieving 100% completion of data protection and security awareness training for all employees and partners by 2026.
- **Third-party Compliance**: Ensuring 70% of contracts include data protection and confidentiality clauses, with a goal of reaching 100% by 2026.
- **Annual Audits**: Conducting regular data protection and IT security audits.
- **Data Breach Response**: Addressing breaches through the **Whistle-blower Policy** and immediate remedial actions.
- **Risk Management**: Identifying and mitigating data-related risks associated with third-party vendors and internal operations.
- **Confidentiality**: Ensuring that third-party data is used strictly within the bounds of contractual obligations.

- **Feedback Mechanism**: Encouraging feedback from employees and partners on data security practices.

Governance

This policy is governed by the **Sustainability (ESG) Council**, which operates under the supervision of the **Sustainability (ESG) Committee** at the Board level. The Council is responsible for overseeing data protection initiatives, compliance, and strategic direction in relation to the organization's data assets.

Policy Review

This policy will be reviewed every three years or as necessary if critical elements need modification.