Himadri Speciality Chemical Ltd

CIN: L27106WB1987PLC042756

INFORMATION SECURITY POLICY

Version	Revision Date	Approved By	Date Approved
Adopted on	January 2023	-	-
V1	10 February 2023	Board	10 February 2023

Information Security Policy

1. Policy Statement

This policy is an overall declaration by Himadri Speciality Chemical Limited (HSCL) of the security objectives and expectations, which will allow utilization of information and information systems for effective and efficient achievement of business goals. HSCL is committed to establish and consistently improve cybersecurity processes and minimize exposure to risks. In continuation with our efforts, we have always strived to ensure best practices are being following within our organization and this policy is formalizing our expectations and practices.

2. Scope and Applicability

This Information Security Policy applies to all HSCL office locations and plants, including employees. Within the scope of applicability of this policy all assets such as, but not limited to, information systems, hardware (such as laptops), software, data, drawings and media in electronic form at HSCL and third-party facilities are covered.

3. Definitions

i) Information: Any communication or representation of knowledge such as facts, data, or opinions in any form, including textual, numerical, graphic, cartographic, narrative or audio visual

ii) Information Security: Protecting information and information system from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability

iii) Information Security Event: An identified occurrence of a system, service or network state indicating a possible breach of information.

iv) Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information system processes, stores or transmits will constitute a violation or imminent threat of violation of security policies and security procedures

v) Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of the likelihood of occurrence and the adverse impacts which would arise if the circumstance or event occurs

vi) Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information

vii) Integrity: Safeguarding the accuracy and completeness of assets against unauthorized information modification or destruction which will ensure information authenticity

viii) Availability: Ensuring timely and reliable access to and use of information

ix) Risk Management: Coordinated activities to direct and control an organization with regard to risk

x) Risk Analysis: Systematic use of information to identify sources and to estimate the risk

4. Information Security Principles

The Information Security Policy will ensure:

- Consistently meeting **expectations of all stakeholders** (investors, suppliers, customers, and employees)
- Ensuring compliance with all applicable **standards, regulatory and legal requirements**

- Apply effective **risk management framework** to identify, manage and mitigate risks associated with HSCL through undertaking a vulnerability assessment
- Protect all HSCL **information and assets** from possible threats which could potentially disrupt the business and functioning of HSCL
- A **backup management system** for creating copies of information which is essential to recover and restore original data in the event of data loss
- Consistently **improve and upgrade technology**, systems, and processes to protect HSCL against known and unknown cybersecurity threats
- Implement **incident management** procedures for detecting, reporting, and responding to incident
- Effectively apply **business continuity and disaster recovery management** controls

5. Compliance to the policy

100% of HSCL employees are required to attend awareness programs on Information Security with regular trainings made available by the management. HSCL will educate employees upon hiring and conduct at least an annual awareness program through emails, posters, and meetings. Employees are encouraged to report any suspicious activity to the Information Security team through (sparamanick@himadri.com). All reported incidents shall be handled in a proper and timely manner with corrective actions being implemented immediately without comprising on the confidentiality, integrity, and availability of information of HSCL.

Information security and cybersecurity are part of the employee performance evaluation as it assesses the employees and whether they are putting the organization at risk, intentionally or unintentionally. The cybersecurity team regularly conducts violation checks on employees' laptops – including email violation, installation, and the use of prohibited software etc. It is the responsibility of each employee to clearly understand and adhere to the Information Security Policy and in case of any violations to this policy, the Management reserves all rights to take disciplinary action, up to and including termination of employment.

6. Governance

The Chief Risk Officer is responsible for overseeing cybersecurity governance as per HSCL's Risk Management Framework. Regular reports pertaining to cybersecurity risks are to be presented from the Information Security team to the Audit and Risk Committee which are further taken to the Board.

The Head of Information Technology is responsible for clearly outlining expectations, providing support in implementing and monitoring progress on safeguarding HSCL information and assets. The Information Security strategy, policy, and cybersecurity programs are to be driven with a top-down approach from the Chief Risk Officer to all business units and function heads further down to all the employees. Business units and function heads are responsible for implementing adequate security policies, process, and controls to protect confidentiality, maintain integrity and ensure availability of all information assets.

7. Exception Management

All exceptions regarding this Policy will be directed to the Head of Information Technology. The exception request will be formally recorded in writing and reviewed by the Head of Information Technology before formally arriving at a decision to approve or reject the exception request. A quarterly summary shall be submitted for review and further action to the Chief Risk Officer. The validity of the exception shall be defined and not exceed one year. An annual review of all accepted exceptions shall be carried out by the Head of Information Technology to identify any changes in risk posed by the exception or to identify alternate controls that could be implemented to reduce the risk.

8. Review

The Policy will be reviewed on an annual basis or in case of any significant changes to check for effectiveness, changes in technology and changes in risk levels that may have an impact on confidentiality, integrity and availability, legal and contractual requirements, and business efficiency.

Sd/-

Anurag Choudhary
Chairman Cum Managing
Director & CEO

Dated: 10 February 2023