Document No	MNG-ISP
Publish Date	26.04.2024
Revision No	2
Revision Date	29.07.2026

INFORMATION SECURITY POLICY

Purpose

Arkem Chemicals B.V. is committed to protecting the confidentiality, integrity, and availability of its information and information assets. Information security is fundamental to maintaining the trust of our customers, business partners, employees, and other stakeholders, while supporting the Company's strategic objectives and sustainable growth.

This Policy establishes the principles and commitments for managing information security across all Company activities. Arkem Chemicals B.V. has established, implemented, maintains, and continually improves an Information Security Management System (ISMS) in accordance with the requirements of ISO/IEC 27001:2022.

The ISMS applies to all information, information assets, business processes, personnel, contractors, third parties, and supporting technologies involved in the Company's operations, including but not limited to import, export, transit, customs clearance, logistics, warehousing, accounting, finance, procurement, engineering, legal, sustainability, quality, reporting, human resources, and information technology.

Policy Statement

Arkem Chemicals B.V. is committed to preventing information security incidents, minimizing the impact of any incidents that occur, and continually improving the effectiveness of information security risk management. Information security risks are managed through a structured and risk-based approach that supports business continuity, operational resilience, and compliance with applicable legal, regulatory, contractual, and customer requirements.

Our Commitments

To achieve these objectives, Arkem Chemicals B.V. is committed to:

- Protecting the confidentiality, integrity, and availability of information and information assets throughout their lifecycle.
- Collecting, processing, storing, sharing, retaining, and disposing of information securely and only for legitimate business purposes.
- Classifying and handling confidential and sensitive information in accordance with established information classification and protection requirements.
- Identifying, assessing, treating, monitoring, and reviewing information security risks using a structured risk management methodology.
- Establishing, maintaining, and regularly testing incident response and business continuity arrangements to ensure timely and effective responses to information security incidents.
- Ensuring that information security requirements are integrated into business processes, projects, system development, and operational activities.
- Defining and communicating clear information security roles, responsibilities, and accountabilities for employees, contractors, suppliers, consultants, and other relevant parties.
- Ensuring that third parties with access to Company information or information systems comply with applicable information security requirements through contractual obligations and, where appropriate, periodic assessments.

INFORMATION SECURITY POLICY

- Providing ongoing information security education, awareness, and training to employees and relevant stakeholders to promote a strong security culture.
- Ensuring that actual or suspected information security incidents are reported promptly and managed in accordance with established procedures.
- Complying with all applicable legal, regulatory, contractual, and customer information security obligations.
- Monitoring the performance and effectiveness of the ISMS through objectives, audits, management reviews, corrective actions, and continual improvement activities.
- Supporting continual improvement by regularly reviewing information security risks, controls, policies, procedures, and best practices.
- Considering information security as an integral part of business planning, investment decisions, digital transformation initiatives, and sustainable growth strategies.

Governance and Responsibilities

The Managing Director is accountable for ensuring the implementation, maintenance, effectiveness, and continual improvement of the Information Security Management System.

Executive Management shall provide the leadership, resources, and support necessary to achieve the objectives of this Policy.

All employees, contractors, consultants, temporary personnel, and third parties with access to Company information or information systems are responsible for complying with this Policy and supporting the protection of Company information assets.

Review and Approval

This Policy shall be reviewed at least annually, or whenever significant organizational, legal, regulatory, technological, or business changes occur, to ensure its continued suitability, adequacy, and effectiveness. Any amendments to this Policy shall be approved by the Chief Executive Officer (CEO) upon recommendation of the Managing Director. Once approved, the Policy shall be published through the Company's approved internal communication channels and, where appropriate, on the Company's external website.

Information Security Objectives

Measurable information security objectives supporting this Policy are established, monitored, and periodically reviewed by Management. These objectives are documented in the **Corporate Strategic Sustainability Targets (MNG-SG)**, which forms an integral part of this Policy and is available at:

https://arkem.eu/strategic-sustainability-goals

Document No	MNG-ISP
Publish Date	26.04.2024
Revision No	2
Revision Date	29.07.2026

INFORMATION SECURITY POLICY

Questions and Reporting

Questions regarding this Policy, requests for guidance, or the reporting of information security concerns or incidents may be directed to the Sustainability Committee via:
sustainability@arkem.com

Prepared by	Checked by	Approved by
OM/ JB	**FM**/ HD	**MD**/ BK