INFORMATION SECURITY POLICY

Arkem Chemicals B.V., as part of a leading and reliable organization in the sector, adopts the electronic information assets of its activities such as import, export, transit, customs clearance and logistics, storage, accounting, finance, purchasing, engineering, law, sustainability, quality, reporting, human resources and information technologies related to these activities, and the information security it uses to protect these assets, in accordance with the ISO 27001:2022 Information Security Management System and implements information security requirements as an integral part of corporate business processes.

Arkem Chemicals B.V. adopts the prevention of internal and external information security incidents, minimizing the impact of possible incidents and increasing the effectiveness of risk management activities as its main goal. In this context, it is aimed to protect corporate digital assets, ensure business continuity and ensure full compliance with legal and regulatory requirements by continuously monitoring, evaluating and controlling information security risks.

For this purpose, in line with our corporate values and sustainable growth strategies and ensuring information security and guarantee business continuity, we are committed to;

- Protect the confidentiality, integrity and accessibility of information and information assets in our business processes,
- Securely collect, process or store third party information for business purposes,
- Ensure that confidential information is managed responsibly,
- Provide training and awareness to ensure that all our employees and stakeholders assume responsibility for information security,
- Increase the awareness and consciousness of all employees and stakeholders about innovations, changes and developments by supporting continuous improvement and development within the scope of the Information Security Management System,
- Identify current and potential risks in order to ensure information security and to evaluate risks related to information security in company operations with an effective information security risk management approach,
- Regularly examining risks, disclosing risks and creating corrective action plans, and conducting risk assessments by third parties when necessary,

- Create and implement an Incident Response Plan (IRP) to ensure rapid, systematic and effective response in case of any unauthorized access, disclosure, loss or violation of confidential information,

- Increase the business continuity and information security performance of all main and supporting business processes; to direct and support these processes effectively and sustainably, in full compliance with business requirements, legal regulations, contractual obligations and relevant legislation,

- Determine the responsibilities of all employees of the company, partners, contractors, customers, suppliers, consultants and any other person or organization,

- Ensure that information security requirements are regularly communicated to all relevant parties/stakeholders,

- Continuous improvement approach is maintained to ensure that Information Security Management System policies and procedures are regularly reviewed and best practices are implemented,

- Carry out all our activities and sustainable growth strategies in accordance with the principles of the Information Security Management System (ISMS); and to consider information security as a priority element of our investment plans in order to protect information assets and reduce risks.

The Managing Director is responsible for the implementation and monitoring of this policy. The Information Security Policy is reviewed by the Managing Director at least once a year in terms of its currentness and effectiveness. Any revisions deemed necessary are submitted to the CEO for approval and put into effect. Once put into effect, it is published on the website and on the company's local network environment (OneDrive) and made accessible to all stakeholders.

The quantitative targets determined by the Managing Director within the scope of our Information Security Policy are defined in detail in the Corporate Strategic Sustainability Targets (https://arkem.eu/strategic-sustainability-goals) document MNG-SG, which is an integral part of this policy.

For detailed notifications and feedback, you can contact the Sustainability Committee via sustainability@arkem.com.