European Responsible Care®
Security Code

Purpose and Scope

The purpose of the European Responsible Care Security Code is to describe the fundamental management practices to protect people, property, products, processes, information and information systems against any kind of criminal, malicious and cyber acts. This encompasses company activities associated with the production, storage, distribution and transportation of products as well as the pertinent liaison with suppliers and customers.

This Code is designed to help companies achieve continuous improvement in security performance using a risk-based approach to identify, assess and address vulnerabilities, prevent or mitigate incidents, enhance training and response capabilities, and maintain and improve relationships with key stakeholders and authorities. The Code will be implemented with the understanding that security is a shared responsibility requiring actions also by other parties such as customers, suppliers, service providers and governmental security agencies. Especially assessing and reducing the global threat of international terrorism can only be effective with the competent support of the responsible national and international counter-terrorism agencies.

Relationship to Chemical Industry Commitments

Security affects many different functions. Besides site security, this topic has become a fundamental element within the supply chain e.g. in transport security and in export and trade controls as well. The Security Code is intended to complement commitments existing in those areas and aims to raise awareness of all involved parties that only close interaction and a regular reassessment of security-related practices will improve the overall security performance.

Responsible Care – Commitment to Sustainability

Responsible Care is the voluntary initiative of the chemical industry to continuously improve its performance on environmental, health, safety and security issues. The Responsible Care ethic helps chemical companies to operate safely, profitably and with due care for future generations.

Responsible Care®
OUR COMMITMENT TO SUSTAINABILITY

cefic

Management Practices

Security management must correspond with the management practices of the individual company. As a guiding principle, the following seven management practices should be taken into account:

1. Leadership Commitment

Senior leadership commitment to continuous improvement through policies, provision of sufficient and qualified resources and established accountability.

The chemical industry's commitment to Responsible Care and security starts at the top.

2. Risk Analysis

Periodical analysis of threats, vulnerabilities, likelihood and consequences using adequate methodologies.

A risk-based approach needs such an analysis first to design an appropriate security plan.

3. Implementation of Security Measures

Development and implementation of security measures commensurate with the risks.

Companies take action for sufficient security processes and will adjust security measures and procedures if necessary.

4. Training, Guidance and Information

Training, guidance for and information of employees, contractors, service providers and supply chain partners as appropriate to enhance security awareness.

As effective security practices evolve, companies will keep pace by enhancing security awareness and compliance through training and guidance.

5. Communications, Dialogue and Information Exchange

Communications, dialogue and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers and government officials and agencies balanced with safeguards for sensitive information.

Maintaining open and effective lines of communication includes steps such as sharing effective security practices with others throughout industry and maintaining interaction with law enforcement officials.

6. Response to Security Threats and Incidents

Evaluation, response, reporting and communication of security threats and security incidents as appropriate and corrective action for security incidents including 'near misses'.

After investigating an incident, the company will incorporate key learnings and will, as appropriate, share those learnings with others in industry and government agencies and implement corrective actions.

7. Audits, Verification and Continuous Improvement

The commitment to security calls on companies to seek continuous monitoring of all security processes.

Companies will periodically review their security programs, processes and measures to affirm those which are in place and will take corrective action as necessary.