7th Responsible Care
Code of Management Practices:

SECURITY CODE

Responsible Care®
OUR COMMITMENT TO SUSTAINABILITY

CICM

SECURITY CODE

CONTENTS

Page

Security Code

- Purpose and Scope 2
- Relationship to Guiding Principles 2
- Relationship to Other Industry Commitments 2
- Management Practices 2

Acknowledgement 6

References 7

RESPONSIBLE CARE®
SECURITY CODE OF MANAGEMENT PRACTICES

Purpose and Scope

The purpose of the Security Code of Management Practices is to help protect people, property, products, processes, information and information systems by enhancing security, including security against potential terrorist attack, throughout the chemical industry value chain. The chemical industry value chain encompasses company activities associated with the design, procurement, manufacturing, marketing, distribution, transportation, customer support, use, recycle and disposal of our products.

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. The Code must be implemented with the understanding that security is a shared responsibility requiring actions by others such as customers, suppliers, service providers, and government officials and agencies. Everyone in the chemical industry value chain has security responsibilities and must act accordingly to protect the public interest.

Implementation of this Security Code is for all members of the Chemical Industries Council of Malaysia (CICM) to further protect the public, our communities and our employees.

Relationship to Guiding Principles

Implementation of the Security Code complies with several of Responsible Care®'s Guiding Principles:

- To operate our facilities in a manner that protects the environment and the health and safety of our employees and the public.
- To lead in the development of responsible laws, regulations and standards that safeguards the community, workplace and environment.
- To work with customers, carriers, suppliers, distributors and contractors to foster the safe use, transport and disposal of chemicals.
- To seek and incorporate public input regarding our products and operations.
- To make health, safety, the environment and resource conservation critical considerations for all new and existing products and processes.
- To practice Responsible Care® by encouraging and assisting others to adhere to these principles and practices.

Relationship to Other Industry Commitments

The Security Code complements, and should be implemented in conjunction with, other management practices that demonstrate the industry's commitment to protecting its employees and the public. Existing management practices that enhance community safety and emergency preparedness, pollution prevention, process safety, employee health and safety, product distribution and product stewardship include security components. Companies regularly should reassess these security-related practices in the spirit of continuous performance improvement.

Management Practices

Each company must implement a risk-based security management system for people, property, products, processes, information and information systems throughout the chemical industry value chain. The chemical industry value chain encompasses company activities associated with the design, procurement, manufacturing, marketing, distribution, transportation, customer support, use, recycle and disposal of our products. The corresponding security management system must include the following thirteen management practices:

1. **Leadership Commitment.** Senior leadership commitment to continuous improvement through published policies, provision of sufficient and qualified resources and established accountability.
   The chemical industry's commitment to security starts at the top. This element calls for each company's leadership to demonstrate through their words and actions a clear commitment to security within their company, from corporate headquarters to our facilities.

2. **Analysis of Threats, Vulnerabilities and Consequences.** Prioritization and periodic analysis of potential security threats, vulnerabilities and consequences using accepted methodologies.
   Using generally accepted tools and methods, companies will conduct analyses to identify how to further enhance security. This process will be applied at chemical operating facilities using any available methods developed by relevant service providers. Companies also will be using tools to analyze the security of product sales, distribution and cyber security. These initial analyses will be conducted on an aggressive schedule then conducted periodically thereafter.

3. **Implementation of Security Measures.** Development and implementation of security measures commensurate with risks, and taking into account inherently safer approaches to process design, engineering and administrative controls, and prevention and mitigation measures.
   Companies will take action when they identify and assess potential security risks. Actions can include putting additional or different security measures into place to provide greater protections for people, property, products, processes, information and information systems. At facilities, actions can include measures such as installation of new physical barriers, modified production processes or materials substitution. In product sales and distribution, actions can include measures such as new procedures to protect Internet commerce or additional screening of transportation providers.

4. **Information and Cyber-Security**. Recognition that protecting information and information systems is a critical component of a sound security management system.
   Companies will apply the security practices identified in this Code to their cyber assets as well as their physical assets. Information networks and systems are as critical to a company's success as its manufacturing and distribution systems. Special consideration should be given to systems that support e-commerce, business management, telecommunications and process controls. Actions can include additional intrusion detection and access controls for voice and data networks, verification of information security practices applied by digitally-connected business partners, and new controls on access to digital process control systems at our facilities.

5. **Documentation.** Documentation of security management programs, processes and procedures.
   To sustain a consistent and reliable security program over time, companies will document the key elements of their program. Consistency and reliability will translate into a more secure workplace and community.

6. **Training, Drills and Guidance.** Training, drills and guidance for employees, contractors, service providers, value chain partners and others, as appropriate, to enhance awareness and capability.
   As effective security practices evolve, companies will keep pace by enhancing security awareness and capabilities through training, drills and guidance. This commitment extends beyond employees and contractors to include others, when appropriate, such as product distributors or emergency response agencies. Working together in this fashion improves our ability to deter and detect incidents while strengthening our overall security capability.

7. **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.
   Communication is a key element to improving security. 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. At the same time, companies understand that their role is to protect employees and communities where they operate, while safeguarding information that would pose a threat in the wrong hands.

8. **Response to Security Threats.** Evaluation, response, reporting and communication of security threats as appropriate.
   Companies take physical and cyber-security threats very seriously. In the event of such threats, companies promptly will evaluate the situation and respond. Real and credible threats will be reported and communicated to company and law enforcement personnel as appropriate.

9. **Response to Security Incidents.** Evaluation, response, investigation, reporting, communication and corrective action for security incidents.
   Companies will be vigilant in efforts to deter and detect any security incident. If an incident should occur, however, the company promptly will respond and involve government agencies as appropriate. After investigating the 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.

10. **Audits.** Audits to assess security programs and processes and implementation of corrective actions.
    Companies periodically will assess their security programs and processes to affirm those programs and processes are in place and working and will take corrective action as necessary. In appropriate circumstances, assessments also will apply to the programs and processes of other companies with whom the company conducts business such as chemical suppliers, logistics service providers or customers.

11. **Third-Party Verification.** Third-party verification that, at chemical operating facilities with potential off-site impacts, companies have implemented the physical site security measures to which they have committed.
    Chemical industry security starts at our facilities. Companies will analyze their site security, identify any necessary security measures, implement those measures and audit themselves against those measures. To help assure the public that our facilities are secure, the companies will invite credible third parties – such as fire fighters, law enforcement officials, insurance auditors and/or federal or state government officials – to confirm that the companies have implemented the enhanced physical security measures that they have committed to implement. In addition, companies should consult with these same parties as enhanced physical security measures are being considered and implemented.

12. **Management of Change.** Evaluation and management of security issues associated with changes involving people, property, products, processes, information or information systems.
    Our employees and our processes contribute to, and rely upon, changes and innovations in products and technologies. As any changes are considered, our companies will evaluate and address related security issues that may arise. This can include changes such as new personnel assignments to installation of new process equipment or computer software or hardware.

13. **Continuous Improvement.** Continuous performance improvement processes entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends and development and implementation of corrective actions.
    Our industry commitment to security calls for companies to seek continuous improvement in all of our security processes. Since practices for addressing security will evolve, it is anticipated that company security programs and measures will evolve, reflecting new knowledge and technology. Companies continually will be tracking, measuring and improving security efforts to keep people, property, products, processes, information and information systems more secure.

Companies will share information on effective security practices within the industry and with external, qualified security professionals. Companies will continue to expand the awareness of and commitment to enhanced security practices throughout the chemical industry value chain. The CICM will continue to provide guidance, including examples of effective member security practices, to assist members in their implementation of this Code, and will periodically review and as appropriate revise the guidance.

Due to the rapidly evolving nature of security issues and related expertise, the CICM will reassess the Responsible Care® Security Code, its management practices and implementation timetable two years after Code adoption or earlier as appropriate. Security Code implementation guidance will be updated as necessary in the interim.

****

Acknowledgements

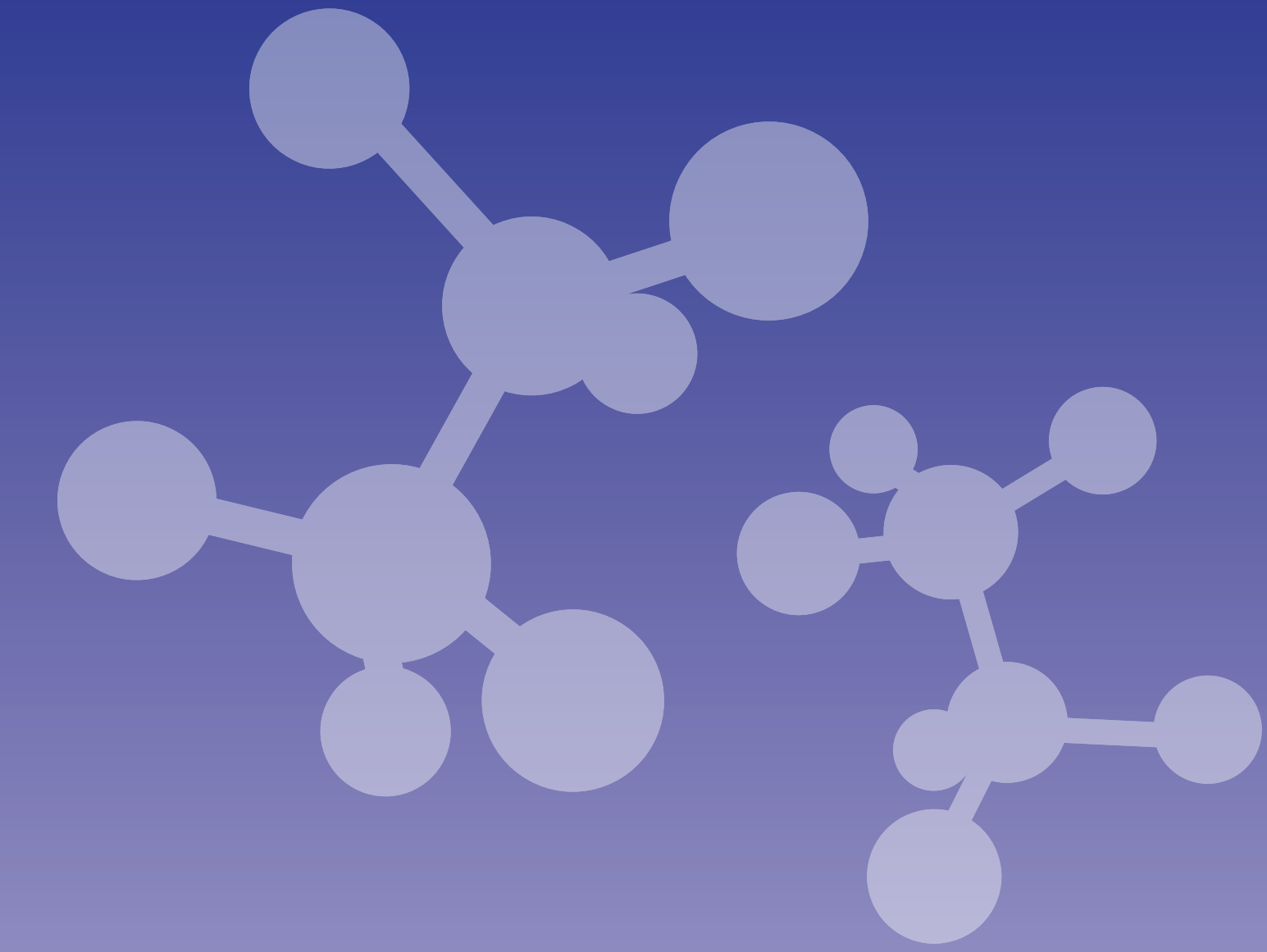
The Chemical Industries Council of Malaysia (CICM) wishes to express its appreciation and gratitude to the CICM Responsible Care Committee and the CICM Security Code Task Force whose guidance, cooperation, commitment, support and assistance made possible the compilation of this Code.

The CICM would also like to record its appreciation to the following persons and organizations for their valuable contributions, expertise and devotion, which had been utmost helpful in the completion of the Security Code.

YH Dato' Muhtar Hashim *Chairman of CICM Responsible Care Committee*	ICE Petroleum Engineering Sdn Bhd
En Zamri Mohd Said *Chairman of CICM Security Code Task Force*	PETRONAS Chemicals Group Berhad
Ir Harminder Singh *CICM RCP Technical Advisor*	
Captain Ayong anak Entili	BASF PETRONAS Chemicals Sdn Bhd
En Mohd Ismafazil Ismail	DuPont Malaysia Sdn Bhd
En Mohamed Mohsin bin Abd Karim	Linde Malaysia Sdn Bhd
Ms Liew Pey Wee	Linfox Transport (Malaysia) Sdn Bhd
En Che Azuri bin Che Yaakub	Orica-CCM Energy Systems Sdn Bhd
En Mohd Razali bin Idris	Tenaga Kimia Berhad
En Yusva Mochtar / En Azmi bin Embi	Chief Government Security Office, Prime Minister's Department
Pn Maslina Daud / Pn Sabariah Ahmad	CyberSecurity Malaysia
En Mazli Hafiz	Department of Environment
En Hafizie Sulkaflee / En Faisal Jusoh	Department of Occupational Safety and Health
Encik Mohd Reza b Azman	Ministry of International Trade and Industry
Puan Saleha Abd Rahman / En Mohd Nazri bin Mustafa	National Authority on Chemical Weapons Convention
En Mohamad Mahathir bin Amir Sultan	LESTARI, UKM

References:

- Security Code of Management Practices by American Chemistry Council (ACC)
- Security Code Checklist by Responsible Care Indonesia (RCI)



Chemical Industries Council of Malaysia (CICM)
Wisma FMM,
No. 3, Persiaran Dagang,
PJU 9, Bandar Sri Damansara,
52200 Kuala Lumpur, Malaysia
Tel: +603-6286 7200
Fax: +603-6277 6714
E-mail: secretariat@cicm.org.my
Web: http://www.cicm.org.my/