AMERICAN CHEMISTRY COUNCIL
RESPONSIBLE CARE®
SECURITY CODE OF MANAGEMENT PRACTICES
Updated and Approved by ACC Board of Directors: November 3, 2021

Purpose and Scope

Following the attacks of September 11, 2001, the American Chemistry Council took action to address stakeholder concerns about security of the nation's critical infrastructure. One such action was the adoption of a Security Code of Management Practices under the ACC's Responsible Care® Initiative. The purpose of the Security Code is to protect people, communities, property, products, processes, information, and information systems by enhancing security throughout the chemical industry supply chain. The chemical industry supply chain encompasses company activities associated with the design, procurement, manufacturing, marketing, distribution, transportation, customer support, use, recycle and disposal of our products.

Since the Security Code's adoption, the threat landscape has evolved with new challenges emerging from a variety of sources. Implementation of the Security Code of Management Practices has enabled American Chemistry Council members and Responsible Care Partners to respond to these challenges and to continually improve their physical and cybersecurity management systems.

This Code is designed to supplement existing security requirements contained within the Responsible Care Management System® (RCMS®) and RC14001® Technical Specifications which help companies achieve continual improvement in security performance using a risk-based approach to identify, assess and address vulnerabilities, prevent, deter, 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, and service providers with support from government officials and agencies as necessary. Chemical industry supply chain participants act accordingly to protect the public interest.

The Security Code also complements regulatory requirements such as the US Department of Homeland Security's (DHS) Chemical Facility Anti-Terrorism Standard (CFATS) & Maritime Transportation Security Act (MTSA) regulations and other government programs. Regulatory standards, by necessity, focus on security for an organization, at an individual facility, and modes of transportation. In contrast, the Security Code addresses issues across ACC member and Partner organizations regardless of their regulatory status. Implementation of this Security Code is mandatory for all members and Responsible Care Partners of the American Chemistry Council to further protect the public, our communities, and our employees.

Management Practices

Each ACC member and Responsible Care Partner company must implement a risk-based security management system. The risk-based security management system will conform to the following management practices:

1. Leadership and Culture.

Senior leadership commits to creating, valuing, and sustaining a strong security culture throughout the organization. Leadership at all levels consistently demonstrates a visible and ongoing commitment and organizational emphasis on fostering continual improvement of security performance across the organization's supply chain.

The organization's senior and other leadership will:

1.1 Demonstrate the importance of security through words and actions, including an understanding of significant risks and their potential consequences;
1.2 Establish and routinely communicate security performance expectations, including measurable goals, objectives and targets;
1.3 Allocate sufficient resources to meet performance expectations;
1.4 Encourage openness in raising concerns and identifying opportunities for improvement in a secure manner;
1.5 Actively promote a visible culture of security excellence across the organization; and,
1.6 Facilitate collaboration of cybersecurity and physical security functions.

2. Security Risk Management

Identify, prioritize, and analyze potential security threats, vulnerabilities and consequences using industry recognized techniques and methodologies. An integrated risk management strategy requires an in-depth understanding of the potential interrelated impacts between cyber and physical functions.

To implement measures to minimize security risks, the organization will:

2.1 Assess and inventory its key physical and cyber assets;
2.2 Understand the threats and risks to its physical and cyber assets, including operating technology, both separately and together, to support informed decision making;
2.3 Communicate, coordinate, and collaborate to develop a common threat landscape and a unified risk strategy;

2.4 Rank and prioritize security risks using industry based and recognized techniques and methodologies;
2.5 Allocate resources to minimize risk exposure;
2.6 Conduct integrated security vulnerability assessments for industrial and non-industrial sites and key assets;
2.7 Develop processes and programs to secure key assets and the enterprise; and,
2.8 Establish a process to regularly re-assesses security risks, considering the changing threat landscape.

3. Implementation of Security Measures

The organization will develop and implement security measures commensurate with identified risks.

When developing and implementing these measures, the organization will:

3.1 Implement, in a timely manner, policies, procedures, programs and physical and/or technological enhancements as appropriate to address the identified risks;
3.2 Consider leading security practices and the experiences of other organizations;
3.3 Address potential risks to business continuity;
3.4 Work with its commercial partners and others in its supply chain to address shared risks; and,
3.5 Align security measures to be compatible with other safety and environmental measures.

4. Documentation.

Documentation of security programs, processes, and procedures.

To sustain a consistent and reliable security management system, the organization will:

4.1 Identify and document key elements of its security management system including, but not limited to policies, procedures, and governance for physical, cyber, corporate, and confidential or proprietary business information;
4.2 Maintain documented information on identified security risks and the methodology used to identify them; and,
4.3 Implement measures to secure data and information.

5. Training and Guidance

Employees, contractors and supply chain partners, as appropriate, are provided with relevant information and made aware of their role in the security management system. Personnel are

made aware of security risks associated with their role and the consequences associated with nonconformity.

The organization will:

5.1 Identify and provide training necessary at relevant levels and functions to support the security management system; and,
5.2 Maintain training records per internal document retention requirements.

6. Security Threat Assessment and Response

Develop, maintain, and continually improve processes to detect, deter, delay, and respond to potential security threats and work to prevent these threats from becoming actual security incidents.

The organization will promptly respond to potential security threats to its people, assets, products, and supply chain by:

6.1 Evaluating and assessing potential threats and impacts;
6.2 Determining the credibility of the potential threats;
6.3 Activating existing security mitigation/response plans and monitoring developments; and,
6.4 Communicating relevant information to internal and external stakeholders, including law enforcement/government authorities where applicable;

In the event a threat becomes an actual security incident, the organization will:

6.5 Initiate existing security mitigation/response plans;
6.6 Take appropriate action, as defined in its existing security mitigation/response plans; and,
6.7 Communicate relevant information to internal and external stakeholders and law enforcement/government authorities where applicable.

Following potential threats and/or actual security incidents, the organization will:

6.8 Conduct a post-threat and/or post-incident response review to identify potential causes, learnings, and opportunities for improvement;
6.9 Investigate the cause(s) of system nonconformities and implement necessary corrective actions;
6.10 Implement necessary corrective actions to improve existing security mitigation/response plans; and

6.11 Share relevant learnings, as appropriate and with appropriate safeguards, to audiences including, but not limited to, law enforcement/government authorities, internal and external stakeholders and/or industry peers.

7. Crisis Management

Integrate security-related scenarios into crisis/emergency management plans to minimize potential impacts to people, communities, operations, and the environment, as well as potential impacts to suppliers, customers and supply chains.

When integrating security-related scenarios into crisis/emergency plans, the organization will:

7.1 Identify reasonably foreseeable scenarios that would activate the organization's crisis/ emergency management plan;
7.2 Determine possible responses to the identified scenarios;
7.3 Define triggers for activation of the crisis/emergency management plan, considering levels of urgency and how to escalate the response if necessary;
7.4 Establish lines of authority and a reporting structure;
7.5 Identify resources needed to support its crisis/emergency management function in the event it is activated; and,
7.6 Plan for both internal and external communications to employees and others working on its behalf, law enforcement/government authorities, members of the public and other key stakeholders.

8. Verification

Organizations conduct verifications of security management system to assess effectiveness.

The organization will:

8.1 Periodically assess the effectiveness of its security management system;
8.2 Document the assessment method used and the assessment's results;
8.3 Take corrective action as necessary; and
8.4 Maintain records as required by compliance obligations or company policy.

Verification may be accomplished through:

- Testing;
- Drills and exercises;
- Auditing;
- External party review; or

- Other means to determine that the security management system meets the organization's security objectives.

9. Management of Change

The organization manages changes that can impact the effectiveness of its security management system. The management of change process may be specific to the security management system or part of an integrated, organization-wide, multi-discipline approach addressing temporary, limited application, or permanent changes.

Changes the organization will consider include, but are not limited to, those associated with:

- Physical operations;
- Technological, operational, cyber, or other systems;
- Organizational structure, leadership or business-related organization;
- Product or service changes; and,
- Security threats or vulnerabilities identified from audits, inspections, tools, or other sources.

10. Continual Improvement

The organization conducts reviews of its security management system, including, but not limited to physical, cyber, and operational technology, supply chain and intellectual property protection programs to confirm it is meeting its objectives and/or identifying opportunities for improvement. The review process may result in revisions, changes or redesign of security management system elements as necessary to achieve its security-related objectives and to reflect current internal and external factors affecting the security management system.

Inputs to the organization's review process may include, but are not limited to:

- Results of internal audits, inspections or verification activity;
- Stakeholder inputs and expectations;
- Technological changes;
- Results of management of change reviews;
- Changes to compliance obligations;
- Identified external excellent practices;
- Threats or opportunities to its security profile;
- Results of exercises, drills or technical outputs; and,
- Threat or incident response investigations or after-action reviews.

Document Control

Version	Modifications	Date
01	Original Version	November 2012
02	Text reformatted with decimal-numbered clauses; enhanced clarity of implementation expectations; and additional detail to cyber-security expectations.	November 2021