الرعاية المسئولة
التزامنا نحو الاستدامة
RESPONSIBLE CARE®
OUR COMMITMENT TO SUSTAINABILITY

gpca
GULF PETROCHEMICALS & CHEMICALS ASSOCIATION
الاتحاد الخليجي للبتروكيماويات والكيماويات

4

SECURITY CODE

Document Number : GPCA-RC-C04
Re-issue Date: January 01, 2018
Revision Number: 01
Prepared / Reviewed by: RC Codes Subcommittee
Ownership: Responsible Care® GPCA
Approval: Dr. Abdul Wahab Al-Sadoun

Acknowledgements

Reviewed and Revised by
Responsible Care Codes Subcommittee

Name	Title	Company
Abdulaziz Al-Mutairi	Team Leader	SABIC
Mark Appleyard	Member	CAMELOT
Kashif Rasheed	Sr. RC Specialist	GPCA

Originally Developed by

Security Code Task Force 04

Original Issue: June 15, 2011

Sayer H. Al-Shammari	TF Leader	SABIC
Jassim Darwish	Member	GPIC
Mansour Al-Dosari	Member	QAPCO
Abdelhamid Belhoula	Member	BOROUGE
Bader Al-Adwani	Member	PIC
Hassan W. Al-Shaikh	Member	SABIC

Table of Contents

CHAPTER ONE

Introduction

History of Responsible Care®

In December 2009, the Gulf Petrochemicals and Chemicals Association (GPCA) Board of Directors formally adopted the Chemical Industry's initiative called 'Responsible Care®'.

Responsible Care® was created in 1984 by the Canadian Chemical Producers' Association, with the clear intent of establishing the following goals:

- Improved chemical processes.
- Enhanced practices and procedures.
- Reduction of every kind of waste, accident, incident, and emission.
- Reliable communication and dialogue.
- Heightened public scrutiny and input.

Responsible Care® has become an obligation of membership in GPCA Member Companies. A central idea behind Responsible Care® is the need to adopt philosophy of continuous improvement. It is not a program that provides a checklist of activities for member companies to implement. It will be improved continually in light of new information, new technology, new expectations, and a constant reassessment of performance and objectives. Responsible Care® is a license to operate.

Management Codes

Responsible Care® is underpinned by GPCA through the implementation of a number of Management Codes as indicated below.

Management Code	Document Number
Community Awareness and Emergency Response (CAER)	GPCA-RC-C01
Distribution	GPCA-RC-C02
Product Stewardship	GPCA-RC-C03
Security	GPCA-RC-C04
Health & Safety	GPCA-RC-C05
Process Safety	GPCA-RC-C06
Environmental Protection	GPCA-RC-C07

Each of the above Codes includes expectations, termed Management Practices. The Management Practices provide specific technical requirements and guidance for Companies to fulfil their responsibilities in terms of Responsible Care® and can be used as a self-assessment tool.

Objective – Security Code

The objective of the Security Code 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, recycling and disposal of our products.

This Code is designed to help GPCA member 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, 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 mandatory for all members of the Gulf Petrochemicals & Chemicals Association to further protect the public, our communities and our employees.

This Code is composed of Management Practices as indicated in Table 1 – Security Management Practices. Individually, each Practice describes an activity or approach to implement the requirements of this Code.

The implementation of the Security Code will help in fulfilling the requirements of the Responsible Care® management system specification RC 14001. Notably, the implementation will help in closing gaps related to security management system development and implementation requirements of the specification, particularly those requiring Security Vulnerability Assessments (SVA) and Security requirements for the entire value chain activities.

Codes of Management Practices Links to RC 14001:2015 Standard

The implementation of the Security Code will help in fulfilling the requirements of the Responsible Care® management system specification RC 14001. Notably, the implementation will help in closing gaps related to security management system development and implementation requirements of the specification, particularly those requiring Security Risk Assessments (SRA) and Security requirements for the entire value chain activities.

		Security Management Practices												
RC 14001 Responsible Care® Elements		SC-1	SC-2	SC-3	SC-4	SC-5	SC-6	SC-7	SC-8	SC-9	SC-10	SC-11	SC-12	SC-13
4.1	Understanding the organization and its context													
4.2	Understanding the needs and expectations of interested parties							X						
4.3	Determining the scope of the EHS&S management system													

4.4	EHS&S management system				X								
5.1	Leadership and commitment	X											
5.2	Policy	X											X
5.3	Organizational roles, responsibilities and authorities												
6.1	Actions to address risks and opportunities						X						
6.1.2	EHS&S aspects		X	X					X	X		X	X	
6.1.3	Compliance obligations (Legal & Other Requirements)		X						X	X				
6.2	EHS&S objectives and planning to achieve them													X
6.2.2	Planning actions to achieve EHS&S objectives													
7.1	Resources	X											X	
7.2	Competence	X					X							
7.3	Awareness						X							
7.4	Communication							X	X	X				
7.5	Documented Information	X		X	X	X			X	X			X	
8.1	Operational planning and control			X	X	X	X					X	X	
8.2	Emergency preparedness and response						X					X		
9.1	Monitoring, measurement, analysis and evaluation	X	X						X	X		X	X	X
9.1.2	Evaluation of compliance												X	
9.2	Internal audit		X								X			
9.3	Management Review										X			
10.2	Nonconformity and corrective action			X					X	X	X			X
10.3	Continual Improvement	X												X

Table 1 – Security Management Practices

Wherever possible these management practices should be included in the member company's existing programs which address the security management requirements. More so, these practices should be incorporated into the existing programs in such a way that these are part of the regular management review cycle.

Chapter 2 includes the Management Practices along with guidance, suggested activities / examples and self-assessment notes that can be used as a self-assessment tool to assist member companies identify gaps and an effective implementation plan to address those gaps.

CHAPTER TWO

Management Practices Guidance, Suggested Activities / Examples and Self-assessment

SC-1: Leadership Commitment

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

1.0 Guidance

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 leadership personnel through to facility personnel.

- Set the Company Security Policy (standalone or integrated).
- Provide leadership, active involvement and support.
- Approve the content and scope of the security risk assessment, which shall be in line with local authority requirements.
- Set and communicate security expectations and goals.
- Identify, provide and allocate all resources needed to meet established goals.
- Develop and implement a management system program for leadership commitment.
- Provide resources for training of security staff.
- Incorporate security objectives into company annual plans.

1.1 Suggested Activities / Examples

Example No. 1

Senior management must identify, provide and allocate all necessary resources such as manpower, budgeting, and security related tools.

Example No. 2

Include Security Objectives, Strategies, Plans and Security Key Performance Indicators (KPIs) in senior / department management meetings. Also, any security issue / concern shall be highlighted during EHS&S management walkthrough.

1.2 Self-assessment

- Is there an approved Company Security Policy in place (standalone or integrated) singed by senior management?
- Does the policy demonstrate leadership, active involvement and support?
- Does the policy approve the conduct and scope of the risk assessment, which shall be in line with local authority requirements?
- Are the security objectives approved and periodically reviewed by senior management?
- Do senior management commit to identifying, providing and allocating all resources needed to meet established goals?
- Do senior management commit to developing and implementing a management system program for leadership commitment?
- Do senior management commit to providing training requirements for security staff?

- Do senior management commit to incorporating security objectives into company annual plans?

SC-2: Risk Analysis

To prioritize and carry out periodic analysis of potential security threats, vulnerabilities and consequences using accepted industry methodologies.

1.0 Guidance

Using generally accepted tools and methods, companies will analyze and identify how to further enhance security. This process will be applied at chemical operating facilities using international best practice. Companies will also analyze the security of product sales, distribution and cyber security. Initial analysis can be conducted on an aggressive schedule then conducted periodically thereafter.

- Prioritize sites, facilities, offices and other locations where the Company operates or distributes product to understand what critical assets need to be secured.
- Conduct security risk assessments using accepted industry methods.
- Select competent risk assessor and qualified team to adequately analyze the security related hazards.
- Establish a process and schedule for reviewing security risk assessment (SRA).

1.1 Suggested Activities / Examples

Example No. 1

All members of the SRA team should understand their roles and responsibilities, including information or activities they are expected to contribute to the overall assessment. The SRA team must include skilled individuals to provide sufficient knowledge, experience and perspective to adequately analyse security related hazards.

1.2 Self-assessment

- Does senior management commit to conducting SRA's?
- Does the SRA priorities all Company locations and activities?
- Is the SRA conducted by a competent risk assessor?
- Does the company conduct SRA's using accepted industry methodology?
- Is there an established process and schedule for reviewing SRA's?

SC-3: Implementation of Security Measures

To develop and implement security measures commensurate with risks, taking into account process design, material substitution, engineering, administrative and process controls, prevention and mitigation measures

1.0 Guidance

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 levels of protection 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, materials substitution, provide adequate manpower and training. In product sales and distribution, actions can include measures such as new procedures to protect internet commerce or additional screening of transportation providers.

- Assign responsibility for security coordination and establish lines of responsibility.
- Perform a security survey to determine the status of current security measures and the particular physical and procedural conditions in which protection must be provided.
- Develop a comprehensive plan for security, based on a thorough security risk assessment.
- Assign responsibility to implement the measures decided upon.
- Establish an implementation schedule and allocate appropriate resources.
- Confirm that measures have been put in place and are working as desired.

1.1 Suggested Activities / Examples

Example No. 1

After completing a security risk assessment, a comprehensive plan will identify any shortfalls between the existing and the desirable security measures. Where additional recommendations may be justified to reduce risk, each measure / recommendation shall be assigned for implementation.

Example No. 2

Define an implementation schedule for recommendations identified during the security risk assessment. The implementation schedule shall identify the required resources and responsibilities. Costs, difficulties and benefits must also be taken into consideration when developing the implementation schedule.

1.2 Self-assessment

- Is responsibility assigned for security coordination and lines of responsibility establish?
- Does the company perform a security survey to determine the status of current security measures?
- Is the required protection level defined according to status of the current physical and procedural measures?
- Is the SRA used as basis for developing the Site Security Plan?
- Does the company assign responsibility for implementing recommendations identified during the SRA ?
- Does senior management establish an implementation schedule and allocate appropriate resources for SRA recommendations?
- Does the company have a system to confirm that measures have been implemented and are working as desired?

SC-4: Information and Cyber Security

Recognition that protecting information and information systems is a critical component of a sound security management system

1.0 Guidance

Companies will apply the security related Management 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 manufacturing and distribution systems. Special consideration shall be

given to systems that support e-commerce, business management, telecommunications, security systems, Industrial Automation and Process Control Systems. 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.

- Conduct cyber-risk assessment for critical assets utilizing a prevailing industry methodology and address all identified risks with the appropriate treatment.
- Exercise caution when creating connections between internal networks and the internet or other company networks.
- Strict adherence to access control policies and procedures including usernames and passwords.
- Consider whether, if warranted, how to isolate or compartmentalize higher-risk systems from the rest of the facility or company network.
- Establish Network Security Boundaries to protect critical information assets that are connected to a network. Implement multi-layer boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (extranets).
- Evaluate vulnerabilities that may be associated with the use of open systems, identity authentication, remote access, network management, wireless communications, enterprise systems and access to process control systems.
- Consider implementing authentication technology commensurate with the risk of information or system exposure, including screening, i.e., background checks for users with privileged access to critical resources.
- Provide appropriate levels of cyber security awareness, training and education for those who are authorized to use and maintain information and process control systems.
- Establish an incident reporting and response plan that describes actions to be taken if and when a suspected or actual intrusion takes place.
- Install the latest malware protection and prevention software and maintain the update regularly.
- All critical systems, applications, databases and network devices must be backed up and periodically tested to ensure in case of major incident or IT disaster the business will be able to resume their services effectively with minimum disruption.
- Information security requirement shall be part of contract for all business partners/vendors who have direct or indirect access to company systems or network to ensure that they are fully compliant with company information security policies requirements, and company will have a right to evaluate their security effectiveness through periodic audits and spot checks.
- A strong change management process shall be implemented to ensure that only authorized and approved changes are implemented in company environment, Information security shall be fully integrated with change process to ensure that new risks with the change implementation are not overlooked.

1.1 Suggested Activities / Examples

Example No. 1

It is recommended to evaluate weaknesses or gaps, i.e., risk is present in information and cyber security protection systems and also the risk assessment shall be conducted before the introduction of new operating systems, application software versions and major applications.

Example No. 2

Appropriate training, awareness and education to be conducted with all users and special training for authorized users including personnel acknowledgment of security policies.

Example No. 3

All critical Information Assets and systems shall have the latest malware protection and prevention software installed and updated regularly.

1.2 Self-assessment

- Does the company conduct cyber-risk assessment for critical assets utilizing a prevailing industry methodology and address all identified risks with the appropriate treatment?
- Is caution exercised when creating connections between internal networks and the Internet or other company networks?
- Does the company ensure strict adherence to access control policies and procedures including usernames and passwords?
- Does the company establish Network Security Boundaries to protect critical information assets that are connected to a network and Implement multi-layer boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools? And Filter inbound and outbound traffic, including through business partner networks (extranets)?
- Does the company have a system to consider whether, and if warranted, how, to isolate or compartmentalize higher-risk systems from the rest of the facility or company network?
- Does the company evaluate vulnerability that may be associated with the use of open systems, identity authentication, remote access, network management, wireless communications, enterprise systems, and access to process control systems?
- Does the company consider implementing authentication technology commensurate with the risk of information or system exposure, including screening, i.e., background checks, for users with privileged access to critical resources?
- Does the company provide appropriate levels of cyber-security awareness, training and education for those who are authorized to use and maintain information and process control systems?
- Is there an established incident reporting and response plan that describes actions to be taken if and when a suspected or actual intrusion takes place?
- Does the company upgrade malware protection and prevention software regularly?
- Does the company implement data backup for all critical systems, applications, databases and network devices and test the backup periodically?

- Does the company include information security requirement part of contract for all business partners/vendors who have direct or indirect access to company systems or network and the company have a right to evaluate their security effectiveness through periodic audits and spot checks?
- Does the company implement a strong change management process to ensure that only authorized and approved changes are implemented in company environment, Information security are fully integrated with change process to ensure that new risks with the change implementation are not overlooked?

SC-5: Documentation

Documentation of security management programs, processes and procedures

1.0 Guidance

To maintain a consistent and reliable security program, companies will document the key elements of their program Consistency and reliability will translate into a more secure workplace and community.

- All documents (hard and soft copy) produced as part of the security program will carry a "Confidential" status. Those responsible for the program or parts of the program shall have access to the appropriate sections. Although all employees and partners have security responsibilities, access to the documented security program shall be restricted
- Issue a directive stating that the company or site will have written security guidelines and clearly assign roles and responsibilities to implement them.
- Develop general security guidelines, naming the types of assets that require protection and the general types of protective measures that are deemed appropriate.
- Develop specific security guidelines, naming the actual material and procedural requirements, such as fence height, employee badging procedures, visitor accompaniment requirements, lighting specifications, etc.
- Develop guidelines for sites in response to varying degrees of threat. For example, determine criteria for high, medium and low threat level facilities.
- Implement guidelines that require security incidents to be documented.
- Ensure adequate and appropriate training for new personnel and refresher training where required.

1.1 Suggested Activities / Examples

Example No. 1

The company is committed to issue written security guidelines, covering all 13 Management Practices.

1.2 Self-assessment

- Does the company issue a directive stating that the company will have written security guidelines and clearly assign roles and responsibilities to implement them?
- Are all documents relating to security classified as confidential and available only to those personnel who have specific responsibility under the program?
- Are there general security guidelines that identify the type of assets that require protection and the general types of protective measures that are deemed appropriate?

- Are there specific security guidelines developed naming the actual material and procedural requirements, such as fence height, employee badging procedures, visitor accompaniment requirements, lighting specifications, etc.?
- Does the company develop guidelines for sites that face varying degrees of threat?
- Is there a guideline in place to ensure security incidents are documented?
- Does the company keep documentation up-to-date so that staff who are not intimately familiar with security operations at the site can ensure continuity of the program when more experienced staff leave?
- Do senior management commit to assure adequate and appropriate training for new personnel and refresher training where required?

SC-6: Training, Drills, and Guidance

Training, drills and awareness for employees, contractors, service providers, value chain partners and others, as appropriate, to enhance awareness and capability

1.0 Guidance

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, where appropriate, such as product distributors or emergency response agencies. Working together in this fashion improves the ability to deter and detect incidents while strengthening overall security capability.

- Ensure that everyone who is assigned specific security responsibilities receives appropriate training, including appropriate responses to potential incidents.
- Establish training as a routine, expected practice.
- Consider using both internal and external personnel as trainers to ensure that employees receive the best training and to promote contact with others in the security field.
- In appropriate cases, provide security and emergency response training to community members and employees of other companies.
- Consider joint training with local emergency responders and law enforcement.
- Keep records of the training provided.
- Develop evaluation criteria to measure the effectiveness of each element of the training program. Review evaluation results to provide feedback to trainers.
- Conduct drills to test effectiveness of preventive measures and response. Use critiques to improve systems as appropriate.

1.1 Suggested Activities / Examples

Example No. 1

Senior management shall ensure an appropriate training program is established for all employees and specific security training is provided to security staff.

Example No. 2

Initial, specific and refresher training shall be evaluated frequently to determine if the necessary knowledge is fully understood. The evaluation shall be used to revise the training program, where necessary and shall be documented. Training shall be evaluated through feedback from trainees and the trainer (using an Assessment Survey Tool or other equivalent methods) to determine if the necessary competency level is being achieved. The feedback shall critique the quality of material

presented, level of technical detail and applicability of the material to their roles and responsibilities. The evaluation shall be used to revise the training and certification program and to continuously improve training methods.

1.2 Self-assessment

- Does senior management commit to ensure that everyone who is assigned specific security responsibilities receives appropriate training?
- Does the company establish training as a routine, expected practice?
- Does the company consider using both internal and external personnel as trainers to ensure that employees receive the best training and to promote contact with others in the security field?
- Where appropriate does the company, provide security and emergency response training to community members and employees of other companies?
- Does the company consider joint training with local emergency responders and law enforcement agencies?
- Does the company have a system to reinforce training in security practices?
- Does the company keep records of training provided?
- Does the company develop evaluation criteria to measure the effectiveness of each element of the training program and review evaluation results to provide feedback to trainers?
- Does the company conduct drills to test the effectiveness of preventive measures and response and use critiques to improve systems as appropriate?

SC-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 agencies, balanced with safeguards for sensitive information

1.0 Guidance

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 the 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.

- Maximize employee awareness of security issues and procedures to increase employees' role in company security efforts.
- When appropriate, share threat information with employees so they can increase their personal safety.
- Develop formal and informal liaisons with local authorities / agencies to improve information sharing, clarify emergency response, track threat conditions and support investigations.
- Develop guidelines for communicating with community groups, including elected officials whilst balancing information needs with security concerns.

1.1 Suggested Activities / Examples

Example No. 1

The use of brochures, posters, the company intranet, meal room table top display cards, briefings and other media to convey information to personnel is recommended to enhance employee awareness of security issues. Establish a variety of means by which employees can report concerns, such as anonymous tip lines, suggestion boxes, a widely distributed security email address, etc.

Example No. 2

The Security Liaison Program involves local and regional law enforcement at multiple levels to ensure support during normal and emergency situations and, along with the security business centres, keep security personnel abreast of the latest developments in chemical industry security. The program is implemented through meetings, coordination of emergency planning and joint activities. This program also includes establishing liaison with appropriate security emergency response organizations.

1.2 Self-assessment

- Does the company have a program / system to maximize employee awareness of security issues and procedures to increase the employees' role in company security efforts?
- Does the company, when appropriate, pass threat information to employees so they can increase their personal safety?
- Are formal and informal liaisons with local authorities / agencies established to improve information sharing, to clarify emergency response, track threat conditions and support investigations?
- Does the company develop guidelines for communicating with community groups, including elected officials, whilst balancing information needs with security concerns?

SC-8: Response to Security Threats

Evaluation, response, reporting and communication of security threats as appropriate

1.0 Guidance

Companies take physical and cyber-security threats very seriously and in the event of such threats, companies will evaluate the situation promptly and respond. Real and credible threats will be reported and communicated to company and law enforcement personnel, as appropriate.

- Regularly evaluate the number and severity of reported security incidents. Communicate any significant increases or decreases in threat levels to upper and line management.
- Upgrade security measures incrementally as the threat level escalates. Review threat escalation with management and obtain their endorsement to enhance security procedures.
- Disseminate pertinent threat information affecting the safety of employees, the operations of the company and the protection of sensitive information.
- Develop procedures for reporting suspicious purchases of, or inquiries about, chemicals or equipment that could be precursors for weapons of mass destruction or that could be used for chemical or biological terrorism.

- Devise and disseminate procedures for responding to bomb threat telephone calls.
- Establish a decision making tree regarding whether to search or evacuate the building.
- Devise and disseminate procedures to examine, analyse and handle suspicious mail and packages.
- Liaise with emergency responders and other appropriate contacts.

1.1 Suggested Activities / Examples

Example No. 1

Each company shall have a defined Environmental Health Safety & Security (EHS&S) Security Incident Reporting System (SIRS). Security incidents may occur within the company complex or nearby and may cause a security threat to the company. Incidents require tracking and analysis to ensure the most appropriate response. This can be achieved through the collection of received and collected reports and monitoring of reliable media. A final report shall be issued defining the rank-grade of threat, recommendations for countermeasures and for further follow-up. Each company shall frequently plan and attend coordination meetings with authorities and other local industries to gain the intelligence required to advise line management.

Example No. 2

The company shall have defined response procedures with different security levels to be applied as soon as there is a threat. Should an incident escalate, the Threat Response Matrix indicates the actions to be taken to ensure the protection of company staff and property at each level.

Security shall review threat escalation with management and obtain their endorsement to implement incremental security upgrades.

Example No. 3

The company shall have a procedures detailing appropriate responses in case of any emergency. The procedures shall include internal parties (staff, safety, security) and external (police, civil defence, neighbouring companies). The company can enter mutual agreements with these external parties.

1.2 Self-assessment

- Does the company regularly evaluate the number and severity of reported security incidents or threats?
- Are any significant increases or decreases in threat levels communicated to upper and line management?
- Are security measures upgraded incrementally as threat levels escalate?
- Is threat escalation reviewed with management and their endorsement obtained to enhance security procedures?
- Has the company established a system to disseminate pertinent threat information affecting the safety of employees, the operations of the company and the protection of sensitive information?
- Is there a procedure for reporting suspicious purchases of, or inquiries about, chemicals or equipment that could be precursors for weapons of mass destruction or that could be used for

chemical or biological terrorism?

- Are there procedures in place for responding to bomb threat telephone calls?
- Has the company established a decision making tree regarding whether to search or evacuate the building?
- Are there procedures to examine, analyse and handle suspicious mail and packages?
- Is there a program / system to improve responses to threats and to liaise with emergency responders and other appropriate contacts?

SC-9: Response to Security Incident

Evaluation, response, investigation, reporting, communication and corrective action for security incidents

1.0 Guidance

Companies will be vigilant in efforts to deter and detect any security incidents. If an incident occurs, the company will respond promptly and involve government agencies as appropriate. After investigating the incident, the company will incorporate key findings and will, as appropriate, share those findings with others in the industry and government agencies and implement corrective actions.

- Develop a process for immediate reporting of security incidents.
- Study security incident records to identify patterns of loss and to identify issues of security concern.
- Develop a process for investigating incidents.
- Consider classifying incidents based on the potential outcome instead of the actual outcome.
- Keep final incident investigation reports on file for at least five (5) years.
- Review final incident investigation reports with all personnel whose job tasks are relevant to the incident findings, including contract employees where applicable.
- Develop a crisis management plan.
- Develop a mechanism to ensure that corrective measures are taken after a security incident.

1.1 Suggested Activities / Examples

Example No. 1

The company shall have a clear / defined security incident reporting system (can be aligned with the safety reporting system). Comprehensive security incident reporting helps to provide the company with an accurate picture of events affecting the company and enables the company to prepare and respond appropriately.

Example No. 2

After any incident the company should adopt a system for communicating that the incident occurred and disseminate investigation findings with all concerned. This communication can be achieved through: meetings, emails, EHS&S alerts and sharing lessons learnt with other organizations. This action will help identify security threats and corrective actions required to prevent them in future.

1.2 Self-assessment

- Is there a process for the immediate reporting of security incidents?
- Does the company study security incident records to identify patterns of loss and to identify issues of security concern?
- Has the company a process for investigating incidents?
- Does the company classify incidents based on the potential outcome instead of the actual outcome?
- Does the company keep final incident investigation reports on file for at least five (5) years?
- Does the company review final incident investigation reports with all personnel, whose job tasks are relevant to the incident findings, including contract employees where applicable?
- Is there a crisis management plan in place?
- Is there a mechanism in place to ensure that corrective measures are taken after a security incident?

SC-10: Audits

Audits to assess security programs and processes and implementation of corrective actions

1.0 Guidance

Companies will periodically assess their security programs and processes to confirm they are working effectively and where weaknesses are identified, will take corrective action as necessary. In appropriate circumstances, assessments also apply to the programs and processes of other companies with whom the company conducts business, such as chemical suppliers, logistics service providers or customers.

- Establish a policy of conducting regular security audits.
- Develop a detailed, comprehensive audit checklist or protocol that covers all key aspects of security, including physical security measures, procedures, documentation (such as security policies and threat or incident reports), cyber-security, product stewardship considerations and management / supervision practices.
- Consult with legal team in the development of the audit program.
- Review previous security audits to identify prior issues of concern. Also, determine whether corrective actions identified in the last report or identified through third-party input or inspections have been completed.
- Conduct personnel interviews, make observations at the site, test the functioning of security equipment and examine documentation.
- Record the specific steps taken in the audit, such as persons interviewed (name and position), equipment tested and documents reviewed.
- Review the audit's preliminary conclusions with the appropriate facility contacts to ensure accuracy.
- Produce a final audit report that clearly specifies issues that require corrective action.

1.1 Suggested Activities / Examples

Example No. 1

Company should establish a policy to periodically review and test the security system to include:

- Planning.
- Fieldwork.

- Audit Report.
- Follow-up Review.

Client involvement is critical at each stage of the audit process. This audit will help proper deployment, identify weaknesses and incorporate lessons learnt.

The Audit may include:

- Security procedures / plans.
- Security structure / organization chart.
- Security incident reporting procedures.
- Security incident report log.
- Site security training practices.
- Security training records.
- Outside law enforcement assistance and coordination plan.

Example No. 2

Any audit, internal or external, should include interviews, observations and system examinations through:

- Conducting scheduled surveys.
- Interviewing concerned parties.
- Examining and testing measures applied and their efficiency.
- Site visits.
- Recording findings.

1.2 Self-assessment

- Has the company established a policy of conducting regular security audits?
- Are there detailed, comprehensive audit checklists or protocols that cover all key aspects of security, including physical security measures, procedures, documentation (such as security policies and threat or incident reports), cyber-security, product stewardship considerations, and management / supervision practices?
- Does the company consult with a legal team in the development of an audit program?
- Does the company review the previous security audit to identify prior issues of concern?
- Has the company determined whether corrective actions identified in the last report or identified through third-party input or inspections are been completed?
- Does the company have a program to conduct personnel interviews, make observations at the site, test the functioning of security equipment and examine documentation?
- Is there a record of the specific steps taken in the audit, such as persons interviewed (names and positions), equipment tested and documents reviewed?
- Does the company review the audit's preliminary conclusions with the appropriate facility contacts to ensure accuracy?
- Does the company produce a final audit report that clearly specifies issues that require corrective action?

SC-11: Verification

Independent verification that, at chemical operating facilities with potential off-site impacts, companies have the physical Security measures that they have committed to implement.

1.0 Guidance

To be implemented as part of their commitment to security, companies will analyse site security, identify any necessary security measures, implement those measures and audit against those measures. To help assure the public that facilities are secure, companies can invite credible third-parties, such as fire fighters, specialist security assessors / auditors, law enforcement officials, insurance auditors and/or government officials to confirm that they have implemented the enhanced physical security measures that they have committed to.. In addition, companies should consult with these same parties as enhanced physical security measures are being considered and implemented.

- Identify verifiers that will be seen as independent and credible to employees, neighbors and other facility stakeholders.
- Determine key points at which to engage verifiers in the facility's security assessment process. Facilities are encouraged to bring verifiers into the process as early a practicable.
- Solicit recommendations from verifiers for improving the facility's security assessment process.
- Assure verifiers view physical security enhancements implemented as a result of the facility's security risk assessment.
- Document that verification has occurred using format appropriate to site/company.

1.1 Suggested Activities / Examples

Example No. 1

The company will invite credible third parties to confirm that they have implemented the enhanced physical security measures they have committed.

Example No. 2

The countermeasure recommendations shall be scheduled and assigned for implementation by company and verified by third-parties.

1.2 Self-assessment

- Does the company identify verifiers that will be seen as independent and credible to employees, neighbours and other facility stakeholders?
- Does the company determine key points at which to engage verifiers in the facility's security assessment process?
- Does the facility bring verifiers into the process as early as practicable?
- Does the company solicit recommendations from verifiers for improving the facility's SRA process?
- Does the company ensure verifiers view physical security enhancements implemented as a result of the facility's SRA?
- Is verification documented using a format appropriate to the site / company?

SC-12: Management of Change

Evaluate and manage security issues associated with changes involving people, property, products, processes, information or information systems

1.0 Guidance

Employees and processes contribute to, and rely upon, changes and innovations in products and technologies. As any changes are considered, Companies will evaluate and address related security issues that may arise. This can include changes such as new personnel assignments to the installation of new process equipment or computer software or hardware.

- Continuously determine and review the threat level as conditions change, and adjust security measures accordingly.
- Learn of, and respond to, changes that may affect the companies security requirements.

1.1 Suggested Activities / Examples

Example No. 1

Establish a process to ensure that security staff are informed at the earliest opportunity of changes to operations and processes.

1.2 Self-assessment

- Does the company have a system / process for continuously determining the threat level and adjusting security measures accordingly?
- Does the company have a system to learn of, and respond to, changes that may affect a Company`s security requirements?

SC-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.

1.0 Guidance

Industry commitment to security calls for companies to seek continuous improvement in all security processes. Since practices for addressing security will evolve, it is anticipated that company security programs and measures will also evolve, reflecting new knowledge and technology. Companies will be continually tracking, measuring and improving security efforts to keep people, property, products, processes, information and information systems more secure.

- Employ a continuous improvement process that follows the sequence "Plan, Do, Check, Act."
- Monitor internal and external security-relevant conditions and trends.
- Develop a sense of employee ownership of site security.
- Provide a confidential system for employees to report security issues.
- Train security and other site personnel to identify and control potential threats and breaches of security.
- Review prevention measures and countermeasures needed to address the identified threats.
- Gather, update, and review security data and revise the site security plan accordingly.
- Conduct internal comparisons (current performance versus past performance) in order to analyze trends.

- Conduct external comparisons through benchmarking against other similar sites.
- Ensure that all requirements of the Responsible Care® Security Code have been met.

1.1 Suggested Activities / Examples

Example No. 1

It is recommended that the continuous improvement cycle consists of these steps: Plan (Develop Strategies), Do (Implement), Check (Evaluate) and Act (Take Remedial Action).

Example No. 2

It is recommended senior management ensure that all requirements of the Responsible Care® Security Code have been met.

1.2 Self-assessment

- Has the company established a continuous improvement process that follows the sequence 'Plan, Do, Check, Act'?
- Are internal and external conditions and trends relevant to security monitored?
- Does the company develop a sense of employee ownership of company security systems and procedures?
- Does the company provide a confidential system for employees to report security issues?
- Does the company train security and other site personnel to identify and control potential threats and breaches of security?
- Has a gap analysis been completed and an improvement plan developed?
- Is there a periodic penetration exercise program?
- Does the company gather, update and review security data and revise the security plan accordingly?
- Is there a system to ensure that all requirements of the Responsible Care® Security Code have been met?

CHAPTER THREE

References

- Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries; ANSI/API STANDARD 780.
- Implementation Guide for Responsible Care® Security Code of Management Practices; American Chemistry Council.
- Risk Management Guide for IT Systems; NIST SP 800-30.
- Industrial Automation & Control Systems (IACS) Security Standards; ISA/IEC-62443.
- GPCA-RC-C04, Issue 15-06-2011.
- American Chemistry Council ACC RC 14001® 2015TITLE: RESPONSIBLE CARE MANAGEMENT SYSTEM® TECHNICAL SPECIFICATION
- American Chemistry Council RCMS®: 2013

Definitions

Asset: An asset is any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to a threat, as well as an owner, although the nature and magnitude of those values may differ.

Consequence: The outcome of an event, commonly measured in four ways—human, economic, mission, and psychological—but may also include other factors such as impact on the environment. Countermeasure: An action, measure, or device intended to reduce an identified risk.

Cyber security: Protection of critical information systems including hardware, software, infrastructure, and data from loss, corruption, theft, or damage.

Mitigation: Ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident.

Physical security: Security systems and architectural features that are intended to improve protection.

Countermeasure: An action, measure, or device intended to reduce an identified risk.
Security risk assessment: A SRA is a risk assessment for the purposes of determining security risk.
Security risk: The likelihood of a threat successfully exploiting vulnerability and the resulting degree of damage or impact.

Threat: Any indication, circumstance, or event with the potential to cause the loss of or damage to an asset. Threat can also be defined as the capability and intent of a threat to undertake actions that would be detrimental to critical assets.

GULF PETROCHEMICALS & CHEMICALS ASSOCIATION
الاتحاد الخليجي للبتروكيماويات والكيماويات

GPCA HQ
P.O.Box: 123055, 1601 and 1602, Level 16
Vision Tower, Business Bay, Dubai, United Arab Emirates
Tel : +971 4 451 0666
Fax : +971 4 451 0777
www.gpca.org.ae