Annual Self-Evaluation Form

Code of Practice

SECURITY

Guidelines for the Implementation of the Management Practices

1. INTRODUCTION

Definition

In view of the rapidly changing security landscape and the heightening of terrorist attacks, security management has become increasingly important within the global business environment. Numerous regulatory and voluntarily initiatives have emerged to enhance the security in the private sector.

In 2017, the Singapore Chemical Industry Council adopted the Security Code as the seventh code of the Responsible Care programme in Singapore. The implementation of the Security Code will complement with the management practices of the other six Responsible Care codes that demonstrate the industry's commitment to protecting its employees and society. Existing management practices that enhance community awareness and emergency preparedness, pollution prevention, process safety, employee health and safety, distribution, and product stewardship may relate to security.

The purpose of the Security Code Management Practices is to help protect people, property, products, processes, information, and information systems by enhancing security throughout the chemical industry value chain. 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.

Annual Self-Evaluation Form

Explanatory Note (how to use the Part 2 and filling blanks in the last 2 columns of the Table):

This Annual Self-Evaluation Form consists of the followings:
- Part 1 of “INTRODUCTION”, and
- Part 2 of “SELF-EVALUATION FORM” that consists 8 management practices for the Security Code.

In part 2, the description of each management practice is in the first column of the Table “MANAGEMENT PRACTICE” and its sub-clauses are in the second column “GUIDELINES FOR IMPLEMENTATION”.

The column “Status” is the result of the evaluation. Company needs to put a tick in the boxes under the “Status” column to indicate if they have met the requirement of the guidelines of implementation, i.e. Yes, No, NA.

The following example illustrates evaluation and filling the result of evaluation:

> *After evaluating a management practice (or its sub-clause), the Company concluded it met all the necessary requirements described in the “Guidelines for Implementation”, the Company should put a tick in the box under the ‘Yes’ column and indicate clearly the index where evidence can be found. On the contrary, if the Company concluded it did not meet the requirements described in the “Guidelines for Implementation”, the Company should put a tick in the box under the ‘No’ column. In the event that the Company does not fall into the category that are applicable for the management practice, the Company should put a tick in the box under the ‘NA’ column.*

Companies shall evaluate in an objective manner if the current practices meet the intent of the clause; in a manner appropriate to the size, complexity and risk of the business.

The annual self-evaluation submission is used by the Country Association (SCIC) to assess progress of Responsible Care implementation and awarding the SCIC Responsible Care Awards. Company is required to attach documents to substantiate and justify their results of evaluation. In view of the large volume of documents likely to be attached with this Annual Self-Evaluation Form, documents should be neatly filed with clear document indexes in one of more hard-paper files for easy referencing. Document indexes pointing evidences should be written in the blanks of the “Document Index” column of the Table to complete the submission. The completed Annual Self-Evaluation Form with all attached documents should be sent to SCIC as a complete set of the annual submission.

Note: Signatories are recommended to work on implementing the guidelines in red first as they are the minimum requirement for Security Code.

2. SELF-EVALUATION FORM

MANAGEMENT PRACTICE	GUIDELINES FOR IMPLEMENTATION*	Status			Evidence/Remarks
		YES	NO	NA	
1. Leadership Commitment *Senior leadership commitment to continuous improvement through policies, provision of sufficient and qualified resources and established accountabilitys*	1.1 Is there emphasis on security as a fundamental part of the overall management system and/or the Responsible Care programme in the form of a written policy or state to all staff and partners?				1. A written policy signed off by senior management. 2. Evidence of Security briefing has been conducted and communicated to all staff.
	1.2 Is there a staff assigned to be responsible for the company's security?				1. Written job descriptions for security related responsibilities. 2. Must have attended at least 1 security related course. 3. Staff with preferably relevant security experience has been recruited.
	1.3 Is there an internal security network and services for your company especially if your company exists more than one site or facility?				1. Company organization chart should include Security function. 2. Have a detail security organization chart which is current.
	1.4 Is there job specific training and qualification for staff dealing with security?				1. Provide security Training Plan 2. Provide Updated Training Record 3. OJT Plan and Refresher Training record
	1.5 Is the security function provided with sufficient resources and with direct reporting lines to the management?				1. List of approved assets for security operations. 2. Security organization chart displayed at the Guard House. 3. Communication protocol is available.
	1.6 Is the security expectations and goals specified and communicated?				1. Annual KPIs for the Security Section.
2. Risk Analysis *Periodical analysis of threats, vulnerabilities, likelihood and consequences using adequate*	2.1 Is there an assessment of the most important asset for the company and for each relevant site? E.g. research facilities,				1. Provide a security risk assessment report endorsed by management. 2. Risk assessment should cover critical assets, identify threats, identify risks and the impact of

methodologies	production plants, headquarters, central computer/computer rooms and infrastructure. Consider the possible impact triggered by theft, loss, damage, disruption, manipulation with malicious intent, rumors or espionage.				each risk.
	2.2 Is the critical chemicals, products, information and processes whose theft, loss, manipulation or release caused by a malicious act could result in significant impacts for the company or the public identified? For example: tank farms, dangerous goods loading facilities, high pressure equipment, process control systems. Consider any relevant assessments that the company has already performed.				1. Provide Register of critical chemicals and processes. 2. Documentation on threat analysis. 3. List of updated signatories 4. Policy on breach to company protocol has been communicated to staff
	2.3 Is the essential security threats for the company, the staff, the assets, the products and the knowhow analysed? Know about the motivation and tactics of e.g. thieves, hackers, frustrated employees, organised crime, violent pressure groups, extremists and terrorists.				1. Evidence of link with Government agencies for update on threats. 2. Reporting system to alert senior management on threats is established.
	2.4 Is the mitigation of residual security risk determined?				1. Evidence that the Risk register is reviewed annually.

Annual Self-Evaluation Form

3. Implementation of Security Measures *Development and implementation of security measures commensurate with the risks.*	3.1 Are the goals of a company specific security concept defined, based on a risk analysis and guided by the principle 'Deter, Detect, Delay and Respond'?				1. Security assurance plan to be reviewed periodically i.e within 3 years' time frame, stating the number of internal/ external security audits and security exercises. 2. Site security plan for each facility to be reviewed periodically i.e within 3 years' time frame.
	3.2 Are there regular site security walk conducted for the company/site to assess the already existing security measures?				1. Conduct quarterly site security walk with Senior management.
	3.3 Are the gaps analysed and addressed by putting additional or modified security measures and check if the implemented measures are effective?				1. Risk Assessment conducted and gaps identified. 2. Security gap and vulnerability closed. 3. Facility security plan has been updated and signed off.
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.*	4.1 Are the staff, contractors, suppliers and service provider aware of and abide to the company's security rules and procedures? This set of information should be a fundamental part of the "Day One" package for new employees and contractors and also for e.g. visitors *(possibly in a shortened version).*				1. Company security rules and procedures have been approved by senior management and communicated to all staff and contractors. 2. Security rules and procedures have been included in the onboarding programme. 3. Basic security rules and procedures featured in the visitor handbook.
	4.2 Is there general awareness on security and information protection via appropriate measures such as presentations, workshops, training sessions, posters, flyers and quizzes?				1. Security awareness activity budget and plan has been approved by management. 2. At least two security awareness activity within the year has been organized and executed.

	4.3 Are the staff involved with critical assets or functions informed in details about the particular security and information protection threats caused not only by outsiders but also by insiders?				1. At least two security training for staff with security responsibilities annually. 2. At least two security exercises per year. (tabletop or live)
5. Communication, 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.*	5.1 Is there means of communication established, possibly tapping the existing platforms within the company? • Inform employees, as appropriate about the current security threats and countermeasures. • Inform management, as appropriate, about lessons learned from security threats, incidents and investigations that have occurred.				1. Evidence of periodic sharing of security incidents and lessons learnt. 2. Mass communication via emails about current security threats and countermeasures.
	5.2 Is there regular information exchange meetings with local/national law enforcement agencies established and ensure that they will inform you immediately about upcoming threats?				1. Evidence of participation in community outreach platforms and networks such as SSWG, NESH, SPF, etc.
	5.3 Is the site security as well as the management and other relevant units informed and will react as required or appropriate whenever there is a change in threat level? Several threat level systems can exist to cause an impact to the company and these can include the national and international systems.				1. Evidence of sharing security updates with employees within the company (e.g via email or employee forum)

Annual Self-Evaluation Form

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".*	6.1 Is there a reporting system established for security issues or extend an already existing reporting process?				1. An approved company security reporting protocol. 2. Evidence of at least two tests carried out on the existing reporting system (eg during tabletop or live exercise).
	6.2 Are incidents evaluated without delay in order to reduce or to limit the impact?				1. Evidence of a procedure on security incident investigation is available in the organization.
	6.3 Is the incident investigation findings and recommendations reported to the management?				1. A procedure/ platform to report incident investigation findings and recommendations to senior management is available.
	6.4 Is there a 'lessons-learned culture' established for security issues within the company and with others, as appropriate?				1. To demonstrate the lesson learnt culture in the organization, via toolbox meeting, mass communication via email, notices and new employee briefing.
7. Audits, Verification and Continuous Improvement *The commitment to security calls on companies to seek continuous monitoring of all security processes.*	7.1 Is security integrated into the "management of change" ("MOC") processes?				1. Key members identified in MOC 2. A written process and procedure have been developed.
	7.2 Are evaluation done on a regular basis for the number and severity of reported company internal security incidents and external security incidents relevant for the chemical industry to ensure that the security system is kept updated?				1. Evidence of collating information on security incidents and analyzing trends in the chemical industry.
	7.3 Are the security processes and procedures reviewed on a regular basis?				1. Evidence of periodic review (within 3 years' time frame) of all security procedures and processes.
8. Information Security *The need to recognize the impact of information security threat to the company and put together a plan to secure confidential information and IT systems.*	8.1 Are the impact of information security treats and its effects recognized by the company?				1. Information Security policy is endorsed by senior management and reviewed annually.
	8.2 Is the network protected against intrusion at the Internet Gateway?				1. Evidence that the network is secured through layered defence. 2. Use of VPN connection from outside organization. 3. Firewall protection for Network is available.

					4. Server is in a dedicated room and is physically secured. 5. Antivirus protection have been updated. 6. Back up of data has been carried out regularly.
	8.3 Is there information protection against unauthorized access? Confidentiality of information is assured and integrity is maintained.				1. Password change policy should be disseminated to all staff. 2. Change of password every 90 days. 3. Have SOPs on authorized IT equipment 4. A clear policy on classification and management of company documents should be written and implemented. 5. Clear-desk policy.
	8.4 Is there awareness of information security among staff?				1. Awareness program on information security to be organized annually involving all employees.

* **Competition Law Reminder** : All discussions between companies for the purposes of implementing this Code must be carried out in compliance with Competition Law. Any questions in this connection should be referred to the respective legal departments of each company.