SUBJECT ICTA RC / RD Security Code of Conduct

DATE 5 September 2018

1. Leadership Commitment

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

Description: The chemical distribution sector´s commitment to security starts at the top. This Code 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 facilities. Examples of topics that might be covered includes:

- Security statement on company website or in vision or mission statement
- Security policy
- Security programmes
- Security training
- Security roles, responsibilities, authorities, and accountability
- Senior Management documented reviews on a periodic basis to ensure implementation through all aspects of operations.

2. Risk Analysis of Threats, Vulnerabilities and Consequences

Prioritization and periodic analysis of internal and external potential security threats, vulnerabilities, and consequences using accepted methodologies.

Description: Using generally accepted tools and methods, companies will conduct and document analyses to identify security risks and measures to enhance security. Companies also will use tools to analyse the security of sites, product sales, personnel and cybersecurity.

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.

Description: Companies will take action when they identify and assess potential security risks. Actions should be proportionate and sustainable. These 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 the 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 the additional screening of contracted hauliers.

4. Information and Cybersecurity

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

Description: 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 production and distribution systems. Special consideration should be given to systems that support process controls, e-commerce, business management and telecommunications.

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 facilities.

International Chemical Trade Association AISBL
A: Hogeweg 16 // The Hague // The Netherlands
E: info@icta-chem.org
T: + 31 70 750 3125
W: www.icta-chem.org

Protection of your data and reputation may include:

- Locking and encrypting computers, using anti-virus software, and using a password manager. Limiting access to that password manager, typically to two people.
- Training employees on social media use, but also on data security protocols, use of personal devices, and reporting incidents. Note that vendors and employees may pose risks, even if unintentional.
- Conducting a mock cyberattack, including simulating an attack and the actions needed as a result. Among the key steps are changing passwords, notifying key stakeholders, and accessing or making backups of data.
- Considering a message in statements, or online, directing consumers to alert business management to possible cybersecurity threats.
- Protecting and securing publishing platforms to protect yourself and prevent the uploading of files that could infect your web site or your web site visitors. Never allow others to upload files without first scanning them for potential risks.

5. Documentation

Documentation of security management programmes, processes and procedures, analysis, audits, and verifications. Include how the site addresses chemical site and transportation security to include conducting a Security Vulnerability Assessment (SVA), if and when applicable.

Description: To sustain a consistent and reliable security programme over time, companies will document the key elements of their security programme. Consistency and reliability will translate into a more secure workplace and community. Companies are expected to regularly review, and where appropriate, revise and redeploy their security plans, and train appropriate personnel at least once every three years.

Questions to ask may include: What do you consider your security documents? Are there documents associated with each component of your security programme? Regarding training, do you have sign-in sheets, certifications, schedules or matrices? For people, have you considered background checks, drug tests, medicals, visitor control acknowledgement, checklist for return of keys/phones, etc. at termination? As for the facility, do you conduct inspections of fences, gates, lights, cameras, etc.? If you have access control, can you print reports that show who had electronic access (such as a fob) at which doors and when?

6. Training, Exercises, and Guidance

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

Description: As effective security practices evolve, companies will keep pace by enhancing security awareness and capabilities through training, exercises, and guidance. This commitment extends beyond employees and contractors to include others, when appropriate, such as emergency response agencies. Working together in this fashion improves the ability to deter and detect incidents while strengthening overall security capability.
Contents could include:

- Procedures for bomb threats, mail and suspicious package handling
- Loading/unloading procedures training
- HAZMAT packaging checklist training
- Contractor policy
- Alerts (emails) cross industry/government training in workgroups
- Requirement that all employees review the security plan and acknowledge by signature that they understand their role

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.

Description: 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 and applicable government agencies. At the same time, companies understand their role is to protect employees and communities where they operate, while safeguarding information that would pose a threat in the wrong hands. Companies need to identify their sensitive information and ensure safeguards are in place.

8. Response to Security Threats

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

Description: Companies take physical and cybersecurity threats seriously. 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, law enforcement personnel, and applicable government agencies, as appropriate.

9. Response to Security Incidents

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

Description: Companies will be vigilant in their efforts to detect and deter any security incident. If an incident should occur, however, the company will respond promptly 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 programmes and processes and implementation of corrective actions.

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

Questions to ask may include: Have you specifically audited your security programmes? If your policy states that you conduct random drug tests, how many have you actually had within the last year? Is that working the way you wanted it to? Were exit interviews completed for all terminating employees? Did you get all your keys/equipment back? Are damaged or defective fencing/gates/lights/cameras being identified in a timely manner and being repaired to your satisfaction?

11. Third-Party Verification

Third-party verification that companies, at chemical operating facilities with potential off-site impacts, have implemented the physical site security measures to which they have committed.

Description: Chemical industry security starts at the 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 facilities are secure, the companies should consider inviting credible third parties – such as fire and rescue services, law enforcement officials, insurance auditors, external third-party audit systems (e.g. Cefic SQAS), subject matter experts and/or government officials –

to confirm the companies have implemented the enhanced physical security measures 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.

Description: 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, the installation of new process equipment, or new 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.

Description: Industry Commitment to security calls for companies to seek continuous improvement in all of their security processes. Since practices for addressing security will evolve, it is anticipated that company security programmes and measures will evolve, to reflect 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.