# SECURITY GUIDELINES

AIGA 003/07

Revision of AIGA 003/04

***Asia Industrial Gases Association***

298 Tiong Bahru Road, #20-01 Central Plaza, Singapore 168730
Tel : +65 6276 0160 • Fax : +65 6274 9379
Internet : http://www.asiaiga.org


# SECURITY GUIDELINES

## Disclaimer





**ASIA INDUSTRIAL GASES ASSOCIATION**
**298 Tiong Bahru Road #20-01 Central Plaza Singapore 168730**
Tel: +65 62760160 Fax: +65 62749379
Internet: http://www.asiaiga.org

## Acknowledgement

This document is adopted from the European Industrial Gases Association document EIGA 907/05/E . Acknowledgement and thanks are hereby given to EIGA for permission granted for the use of their document.

**Table of Contents**

## 1 Purpose

- To address the specific risks for the gas industry due to:

  threatening phone calls / mails
  theft
  fraud and pressure groups
  sabotage
  vandalism
  bomb threats
  terrorism (incl. bio terrorism)

- To give guidance for deterrence / delay / detection of these criminal acts.
- To deal with consequences of such events.

## 2 Scope

- fixed installations
- storage in portable tanks and cylinders
- excluded from the scope are IT security and security of individual persons e.g. by kidnapping

## 3 Risk categories

The first stage in assessing the security risks for a location is to recognise the vulnerability of a site to attack or entry by unauthorised persons. General risks such as theft, arson and vandalism are common to all locations. Some sites will have more specific risks such as terrorism.

In common with other Risk Assessment methodologies the key requirement is to assess the severity of the consequences of a security failure in terms of death, injury, loss or damage together with the probability of it happening.

### 3.1 High risk

- Seveso II top tier sites
- storage of toxic gases in bulk (e.g. $Cl_2$, $SO_2$)
- storage of highly toxic gases in cylinders
- storage of ammonium nitrate
- CO pipelines

### 3.2 Medium risk

- Seveso II lower tier sites
- bulk storage of $NH_3$, $N_2O$, LPG, $GH_2$, $LH_2$, $C_2H_2$
- storage of calcium carbide
- storage of >1000 t LIN, LAR, $LCO_2$
- $H_2$ pipelines

## 4 Risk assessments

It is recommended that AIGA members conduct their own risk assessments and determine appropriate measures. Security risks and steps for their minimisation may vary in countries, for individual companies or even individual facilities.
Risk assessments should take into account:

- properties and quantities of products that need to be protected
- threats that may be posed against assets
- likelihood and consequences of attacks against those assets.

Worst case scenarios should reflect possible events linked to security matters if requested by competent authorities. However they may not in all cases allow for assessing all threats and appropriate counter measures.

Having undertaken a risk assessment, businesses can then consider

- avoiding the risk
- reducing the risk
- transferring the risk
- accepting the risk

## 5 Security measures

The following list shall serve as an orientation. Measures will not only be based on risk evaluation but also on economic aspects and common sense.

### 5.1 Management Responsibility

It is recommended that each location appoints a manager to take responsibility for all security issues. He should

- Manage security issues at the site and carry out instructions to meet specific needs
- Receive reports on security breaches, investigate and keep a record
- Regularly review security procedures and raise the levels of personal awareness
- Ensure contingency plans are in place

### 5.2 Housekeeping

Security is helped by good housekeeping particularly in respect of the following recommendations

- Keep store cupboards locked
- Have a “clear desk” policy particularly in relation to sensitive material
- Keep laptop computers out of site in a locked cupboard when not in use
- Keep yard areas clear of rubbish and unnecessary equipment
- Keep high risk items under effective control and secured appropriately
- Keep all combustible material away from externally accessible fences or walls

### 5.3 Perimeter protection

The aim should be to prevent unauthorised access and to protect the assets. Perimeter fences and walls have the following uses:

- to set out the boundary of the premises
- to assist in controlling entry to and exit from the premises at particular points
- to deter trespassers
- to provide the means of mounting electronic intruder systems.

Perimeter boundaries can be fences. The most common types are chain link, weld mesh, steel palisade and walls. Fences should be 2m high, well maintained and checked regularly for signs of intrusion. Additional protection can be afforded by an intruder repellent barrier of 1m in height. This can be a reverse angled barrier with barbed protection to make it difficult to climb.
There should be the minimum number of breaks in the perimeter fence or wall. Gates used to control these breaks should be to a similar security standard to the fence or wall itself. Unsupervised gates must be kept locked and inspected frequently. Hinges should be designed to resist removal and the ground clearance should be no more than 50mm.
Good and properly maintained lighting will greatly increase the chance of detecting and deterring criminals. It is a highly cost effective security system. All possible ways of entry and exit for intruders should be lit. This means supplying extra lighting where required to cover doorways, loading and unloading areas and vulnerable windows at ground level.

Measures can be taken to enhance security of buildings and high risk areas. These include window/door locks, grilles and creating locked caged facilities.

### 5.4 Access control

The access of staff, visitors, contractors and their vehicles should be regulated. All personnel should be encouraged to challenge anyone not known, unaccompanied and not wearing a visitors pass.

Recommendations for entry and exit standards are as follows:

- All employees should have an identity card with a portrait photograph
- Visitors should be issued with and display an identity pass. They should be accompanied for the duration of their visit
- A procedure should be in place to record visitor details e.g. name, address, date, person visiting and arrival/departure time
- Physical barriers should be installed at vehicle entrances to prevent uncontrolled access

Parking areas should be separated where possible to restrict access to goods and storage areas to those needing it.

There should be good control of keys including
- Records of key numbers, names and holders
- Communal keys kept in a locked cabinet and signed in and out

### 5.5 Building Security

The Risk Assessment should determine the doors which must be secured and standard of lock to be employed. Similarly ground floor windows which could provide access should be considered for fitment of locks or access inhibitors.
Storage sheds or units housing valuable items should be secured with heavy duty padlocks.
It is recommended that the details of all IT equipment (make model serial number) is recorded and checked regularly to ensure items are still available and in the right place.

### 5.6 Electronic security systems

The application of electronic systems in support of physical security equipment deters criminals from attacking facilities, and in the event of an attack can summon a response. Alarms designed to detect intruders are the most basic and well known type of security system and their very existence deters some criminals. However, alarms are of little use if they are not monitored and supported by an effective response. Close circuit television (CCTV) aims to deter crime through fear of detection and identification. More sophisticated types include cameras that can react automatically and intelligently to intrusions.
CCTV systems are especially useful for unmanned sites, monitored from remote locations.

### 5.7 Hiring / employment practices

This applies to permanent as well as temporary employees.
It is recommended to install a pre-employment screening system and to develop and implement a security awareness program for employees. For more details see section 5 of reference no. 1.

### 5.8 Contractor & contractor personnel screening

Security aspects should be contained in the selection criteria.

### 5.9 Hazardous and toxic materials

The necessity of having hazardous materials in stock shall be checked. Also make use of possible minimisation of stored quantities.
Particular consideration should be given to the potential for theft of highly toxic and toxic products for

drug use etc. Also procedures are needed to deal with intentionally disguised cylinders.

### 5.10 Emergency procedures

Decisions on whether and how to evacuate an area in case of threat or attack should be contained in the Emergency Plan.
Calculations for gas dispersion based on credible worst case scenarios should be available to assess what procedure is appropriate.
Specific cases are listed in reference no. 1 section 8.D.

### 5.11 Product sale policy

As part of product stewardship a sale policy for high risk products (especially highly toxic gases) shall be in place. It has to be based on a chemical hazard evaluation. Basic parts are:

- ensure that the customer has a valid reason to purchase toxic products
- verify that the person collecting cylinders with toxic gases is a known customer or can identify himself / herself
- care for customer awareness; besides the obligatory material safety data sheet warnings concerning misuse of gases shall be given.
- Complementary provisions are contained in AIGA 043/07 “Transport Security Guidelines”.

## 6 Conclusion

Based on the guidance given in this publication AIGA member companies should establish their own security rules and define measures.
They are advised where appropriate to cooperate in national industrial gas associations, chemical industry associations and with local authorities.
It is recognised that our industry is not able to stop terrorist attacks in all cases. Besides taking the recommended measures it is important to raise awareness about security with all employees.

## 7 References

1. Security of dangerous loads
   UK Working Party on the transport of dangerous goods
   WP/TDG (01).218 Rev. 1, 28 Sept. 2001

2. CGA – P50 Site Security Guidelines

3. Site Security Guidelines for the U.S. Chemical Industry, October 2001
   *Source:*
   *American Chemistry Council, www.americanchemistry.com*
   *The Chlorine Institute Inc., www.cl2.com*

4. SEVESO II
   *Source:*
   *EC Directive : Seveso II Directive 96/82/EC amended by 2003/105*