



AIRFREIGHT INDUSTRY MINIMUM SECURITY STANDARDS (AIMSS)

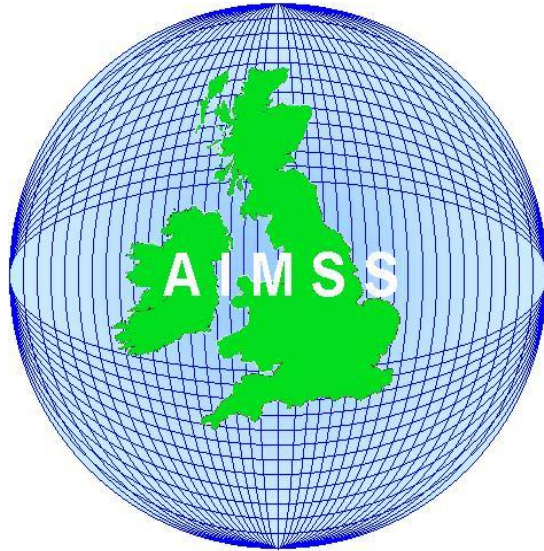


# AIRFREIGHT INDUSTRY MINIMUM SECURITY STANDARDS FOR CARGO

## VERSION 2

November 2007

# **AIMSS Accreditation Self-Assessment Template**



## **AIMSS Accreditation**

### **Notes for Persons Applying for Accreditation**

# Notes for Persons Applying for Accreditation

## Introduction

Welcome to the Airfreight Industry Minimum Security Standards (AIMSS) accreditation guidance. This document is intended to assist those involved in the self-assessment survey of establishments involved in the airfreight industry.

Recent high profile criminal activity in and around cargo handling and transportation has highlighted a need to improve security and to this end, the police and members of the industry have identified AIMSS as the way forward.

AIMSS accreditation will last for a period of two years from the date of validation and the period will be shown on the Certificate of Accreditation. (Where a company fails to meet the AIMSS standards required by its accreditation, the Principal Accreditation Officer may suspend or withdraw the accreditation. The appeals procedure will apply to case of accreditation withdrawal).

Please complete the self-assessment form as fully as possible. This document should be available to the Crime Prevention Officer (CPO) conducting the survey for accreditation.

Please contact your local police station to make an appointment with the CPO for the accreditation survey. Should you have any difficulties please check the AIMSS website ([www.aimss.info](http://www.aimss.info)) for contact numbers.

## The Self-Assessment Template

The AIMSS document provides a set of recommendations for industry to improve security measures in relation to their operations. The document is divided into four parts:-

- Warehouse Security
- Transportation of Valuable and Vulnerable Cargo
- Ground Transport Security
- Security of Information

As can be seen from the headings the survey that needs to be conducted will examine processes as well as the physical security measures in place. To assist you a self-assessment template has been created. The template is intended to serve two purposes. Firstly, to provide a guide for the operator to see if he meets the criteria for AIMSS Accreditation and secondly, to provide the crime prevention officer with a starting point for an accreditation survey.

Within the self-assessment document there are two components, mandatory fields and supplementary fields. The mandatory fields are marked with an 'M'. As you would expect the mandatory components are absolutes. Only sites and areas of operation that have all the mandatory fields will be eligible for accreditation. If you do not meet all the mandatory fields it is important that you contact your CPO in order to address the deficiencies in the mandatory fields. Alternatively, additional information is available on the AIMSS web site.

The supplementary fields are areas where the crime prevention officer will offer advice and make a decision based on the surrounding circumstances.

If you have any queries or need further information or advice please see the AIMSS web site at [www.aimss.info](http://www.aimss.info) .

# AIMSS ACCREDITATION

## Self-Assessment Survey

Name of Company Surveyed:

---

Address of Premises Surveyed:

---

---

---

---

Details of Person Responsible for AIMSS Enquires:

---

Contact Details:

---

Person Conducting Survey:

---

Contact Details:

---

# AIMSS ACCREDITATION

## Self-Assessment Survey

Fields marked with an **M** are mandatory fields and must be complied with in order to receive AIMSS Accreditation. Fields not marked with an **M** are highly recommended. If in any doubt, please refer to your local police crime prevention adviser for advice.

<u>Sections</u>	<u>Page</u>
<b>Warehouse Security</b>	30
Access Control and Staff Identification	30
Security of Premises	31
Collection Of Freight	33
Training	33
Auditing	34
<b>Ground Transportation</b>	34
Driver Requirements	34
Vehicle Requirements	35
Journey Security	35
<b>Security of information</b>	36
General Issues	36
Pre-Alert Messages	37
<b>Vetting and Recruitment</b>	37
(See also Appendix 'A')	

## Warehouse Security

### Access Control and Staff Identification

Main Doc Ref No.	Accreditation Criteria	M	Pass	(Notes)
1.1(a)	Access control processes both during and outside normal operating hours to ensure access is granted only for authorised supplier, employees, and visitors.	M		Use of staff ID cards and visitor passes will enable unauthorised persons to be identified quickly. Passes should only be issued to persons on production of a valid form of identification.
1.1(b)	Security controlled access points (e.g. numeric keypad locks, guard, receptionist, card access system or intercom with CCTV	M		Details of visitors entering the facility should be recorded. Only staff and persons who have a valid visitor's pass should be allowed access to restricted areas. It is important to bear in mind that if a wall does not reach the ceiling, a door lock system provides little security. CCTV covering the area will allow remote monitoring of an access point and record details of all activity in that area.
1.1(c)	Where a card access system is used, a minimum 30 days record of use must be retained.	M		The company needs to keep a list of authorised users and access to the equipment needs to be restricted to those listed. Staff who are required to access the card access system functions need to be trained to an appropriate level. There must be restricted access to card access system functions and a quarterly review of card access reports. Attention needs to be paid to staff entering on days off or out of working hours etc.
1.3(a)	ID Badge policy for visitors/ contractors in place.	M		All visitors must be issued with an ID badge and wear it at all times whilst in the establishment.
1.3(b)	Employee ID picture badges (showing an expiry date) must be issued, carried and ready for inspection at all times whilst on company premises.	M		Local instructions need to be in place to ensure that badges are carried. Ideally, signs informing staff of the need to carry badges and to challenge any person not known to them should be displayed in the warehouse area.
1.4	Unaccompanied admittance to cargo handling and storage areas must be restricted to authorised staff only.	M		Any visitors to the site need to be escorted and should not be allowed access to vulnerable areas.

## Security of Premises

Main Doc Ref No.	Accreditation Criteria	Pass	(Notes)
2.1(a)	All external dock / warehouse doors must be kept shut unless required for operational purposes. Access must be controlled through open doors.	M	A workforce instruction needs to be in place to ensure compliance with this component.
2.1(b)	All external doors must be covered by CCTV.	M	Cameras should be placed in areas where they cannot be obstructed by high-sided vehicles/vegetation etc.
2.1(c)	Recorded CCTV coverage of break / build, storage and loading / unloading areas	M	There may be an area or areas set aside for these functions. The Operational Requirement will dictate which type of CCTV is used
2.1(d)	External and internal lighting levels must support high quality CCTV images and recordings.	M	Lighting is an important addition to CCTV. Flood lighting is not always the most appropriate form of illumination. Consideration must be given to ensure that lighting does not adversely affect the CCTV system.
2.1(e)	Dock doors illuminated externally at night	M	See above
2.1(f)	CCTV system should be able to view sides of the facility		If the sides of your premises contain doors or windows they are vulnerable. Consideration should be given to this area.
2.2(a)	All external doors must be alarmed and linked to a monitored alarm system in premises that do not operate 24 / 7	M	It is important that the alarm system can be zoned or individually isolated. This allows closed / locked doors to remain alarmed when other doors are open.
2.2(b)	Restricted access to any installed alarm system	M	Only authorised to have access to alarm systems and records. Each key holder must have their own individual alarm access code.
2.2(c)	Remote monitoring of any installed alarms to police or security contractor as per the requirement of the ACPO policy	M	Alarms including panic alarms should be connected to a central service provider system in addition to any local activation protocols. Additional connection via GSM is highly recommended.
2.2(d)	Alarm systems fitted inside the warehouse must be set when employees vacate the facility		This facility is particularly important in vault type areas. This must be considered in conjunction with the external door and window alarms.
2.2(e)	Manned security-monitoring post 24/7 should be secure from attack		If the premises are a 24-hour operation this facility should be on site.

Main Doc Ref No.	Accreditation Criteria		Pass	(Notes)
2.2(f)	Any windows or other openings in warehouse walls must be secured by steel bar / mesh (or any other appropriate security material or product).	M		Any protection for windows needs to be well maintained and appropriate to the risk in that particular area.
2.2(g)	Ground floor warehouse windows protected by anti-ram posts or other physical barrier.			Consideration should be given where appropriate to windows that are vulnerable to ram raid attacks.
2.2(h)	Dock doors and exit doors should be designed to prevent or delay forced entry by using portable hand held tools or ramming by vehicles.			Many dock doors are of the roller door type. Reaching this level of security may be difficult. However, anti-ram posts/ ramps must be considered for the any areas where a vehicle can gain access.
2.2(i)	Exterior walls should be designed to resist penetration by removing building fabric, cutting or ramming by vehicles.			Any redesign, strong room, or secure areas should meet this standard.
2.2(j)	Assets stored on site in a vault area for more than two hours should have restricted access – (High grade security mesh/wall, alarmed and CCTV).			This is an ideal solution and should be considered, if not already in place. However, these assets could be placed on high rack storage monitored by CCTV, this would be acceptable.
2.2(k)	Assets caged on site for more than six hours – (chain link cage with roof or similar, padlocked, CCTV coverage)			As above.
2.4(a)	Procedures for random inspection to control rubbish removal from premises must be in place.	M		Regular removal of rubbish is important. Security or managerial staff should accompany persons engaged in this job on an infrequent basis to reduce the risk of goods being left in the rubbish for later collection.
2.4(b)	A policy must be in place to enable searches to be carried out on persons and vehicles in cargo handling and storage areas.	M		Searches should be conducted on a frequent but irregular basis. Details of anything found should be recorded. Paperwork or photocopies may be as important as actual goods.
2.4(c)	Containers such as coolers, lunch boxes, and personal bags should not be allowed in the warehouse. All personal containers should be subject to search when being removed from the premises.			Wherever possible the staff recreation/ locker rooms should be separate from the main warehouse. Employees should pass through a security check area before entering or leaving the premises.
11.1(a)	CCTV must be in good working order and fit for purpose for which it was installed. See CCTV Data Protection Guidance at <a href="http://www.aimss.info">www.aimss.info</a>	M		Regular maintenance of CCTV and alarm systems can prevent expensive repairs / replacement at a later date.

Main Doc Ref No.	Accreditation Criteria		Pass	(Notes)
11.1(b)	All CCTV images are recorded in real time, appropriate to the Operational Requirements. (As per HO Manual)	M		See CCTV Guidance at <a href="http://www.aimss.info">www.aimss.info</a>
11.1(c)	Regular maintenance plan of the CCTV system must be in place	M		As above

### Collection of Freight

4.1(a)	A written procedure must be in place regarding the collection / delivery of cargo. A voluntary thumbprint scheme should be in place for drivers collecting cargo.	M		All drivers delivering or collecting cargo should be checked for appropriate driver identification/ authorization at reception and a record of their vehicle registration kept. At the point of service warehouse staff should confirm driver and vehicle details.
--------	---	---	--	--

### Training

Main Doc Ref No.	Accreditation Criteria		Pass	(Notes)
5.1(a)	A consignor's Security Policy Statement must be available and communicated to all employees.	M		This document should be readily available and highlighted during training etc.
5.2(a)	Robbery response safety training for all dock, warehouse, Security, and reception employees.	M		A document detailing procedures needs to be readily available.
5.1(b)	Procedures in place to routinely test and service security systems	M		Regular maintenance of security equipment and systems can prevent expensive repairs / replacement at a later date.
5.1(c)	Security incident reporting system and method of tracking local security incidents.	M		This document may become evidence in any police investigation. Full details should be included in any report. Management should be informed of any emerging trends or significant incidents immediately.
5.1(d)	A database of emergency contact numbers detailing local management and customers must readily be available for supervisors and managers.	M		Wherever possible this should be available on a computer and password protected.
5.1(e)	Regular CCTV / Alarm training must be available for appropriate personnel	M		Wherever possible this should be on the system installed and password protected.

## Auditing

Main Doc Ref No.	Accreditation Criteria	Pass	(Notes)
6.1(a)	Locally documented procedures for handling cargo must be in place - including auditable damage and irregularity reports and a procedure for communicating security incidents to consignee (or consignee's agent).	<b>M</b>	In addition all staff should be aware of the procedures and a copy should be available for inspection by supervisors and the buyer.
6.1(b)	CCTV must be recorded as per the operational requirement; records and CCTV recordings must be kept in relation to system alarms.	<b>M</b>	The need to keep records will assist in post event evidence gathering and assist in the development of a more robust system. (e.g. where there have been a number of false alarms more appropriate solutions can be identified. Also faults can be identified and rectified quickly.) If an incident is detected the data must be downloaded immediately for post incident investigation
6.1(c)	Auditable process for timely reporting of incidents of lost or missing cargo must be in place. Incidents of missing cargo to be reported by the handler to the consignee (or consignee's agent) as soon as practicable.	<b>M</b>	This document may become evidence in any police investigation. Full details should be included in any report.
6.1(d)	Access to all keys must be controlled and auditable.	<b>M</b>	There should be a booking in and out system for the use of all keys. This provides an audit and accountability trail. All staff should be aware of the company key policy.

## Ground Transportation Driver Requirements

Main Doc Ref No.	Accreditation Criteria	Pass	(Notes)
7.7(a)	Drivers must be fully conversant with the company's security policies and procedures.	<b>M</b>	The company's security policies must reflect the minimum standards identified in the AIMSS document in relation to ground transport.

## Vehicle Requirements

Main Doc Ref No.	Accreditation Criteria	Pass	(Notes)
8.1(a)	Solid top, hard sided, locked cargo doors, or reinforced soft-sided trailer must be used for the transportation of vulnerable goods. (See Section 8 of AIMSS document for a definition of vulnerable).	<b>M</b>	It is important that the appropriate vehicle is used for the goods to be transported. If the handler has concerns in relation to the vehicle being used he should contact the shipper to ensure that they are happy with the transport being used.
8.2(a)	All vehicles must be fitted with a functional immobilization device.	<b>M</b>	Drivers should be aware of how all security devices are activated and deactivated. Instructions should be available to all drivers.

## Journey Security

8.2(b)	Vehicles and trailers must be sealed using appropriate tamper evident seals.	<b>M</b>	Auditable procedures must be in place for the secure storage, issue, and recording of seals. Seal numbers must appear on the appropriate shipping documentation.
9.8(a)	There must be a two-way voice communications system between the driver and his base. An information reporting protocol must also be in place.	<b>M</b>	Drivers should be aware of the immediate actions in the event of an unscheduled event. Training should be provided in relation to breakdown procedures, hijack, and hostage situations.
9.6(a)	Only use routes, schedules, and planned stops negotiated in advance and approved.	<b>M</b>	Any deviation from the approved routes should be notified immediately.
9.2(a)	There must be documentary records of shipping details (time, date, driver, shipping / receiving personnel, shipment details, and quantity).	<b>M</b>	
9.1(a)	The driver must be present during the loading / unloading operations to ensure the integrity of the shipment and agree the piece count (where appropriate).	<b>M</b>	The driver is the link between the point of loading and unloading. The cargo is his/ her responsibility throughout the journey to the point of delivery. This continuity reduces the risk of driver blamed theft.
9.1(b)	Company procedures should require that the loading of vehicles and trailers should take place as near as practicable to the departure time of the load.		Unattended vehicles and trailers should not be used for the storage of cargo.
9.1(c)	Vehicles and trailers should be fitted with tracking devices.		This will enable companies and police to locate vehicles and trailers at all times.

## Security of information

### General Issues

Main Doc Ref No.	Accreditation Criteria	M	Pass	(Notes)
10.1(a)	Access to paperwork and information relating to shipments of cargo must be restricted to employees who 'need to know' to allow them to carry out their job effectively.	M		Only those who have an operational need to information should be allowed access. Documents should be stored in a secure environment and completed paperwork should be returned to the secure area as soon as possible. Photocopying of documents should be monitored and a record kept.
11.1(d)	Restricted access to CCTV system functions	M		The company needs to keep a list of authorised users and access to the equipment needs to be restricted to those listed. Staff who are required to access the CCTV equipment need to be trained to an appropriate level.
11.1(e)	Minimum 14 days retention of all recorded CCTV images and held in secure storage area	M		The recording system must be capable of recording for 14 days with movement detection and various frame rates to keep the level of storage space down. Recommended 31 days where possible.
11.1(f)	A termination of employment procedure must be in place that ensures the return of ID's, access cards, keys and other sensitive information from employees and contractors.	M		These procedures must form part of the employee or contractor's conditions of service. Any access to IT equipment must be immediately suspended if a member of staff is suspended pending investigation or dismissed. Following dismissal any access rights must be terminated immediately.
11.1(g)	A record should be kept relating to previous employee for a reasonable period of time after the termination of their contract.			Over time there may be the ability to share this information with other companies within the industry. Ensure that any information held complies with the Data Protection Act.
11.2(a)	CCTV must be used and linked to the main CCTV system to monitor all counter areas where documents are exchanged.	M		
11.3(a)	Collection of VAL / VUN air waybills must be auditable.	M		

## Pre-Alert Messages

Main Doc Ref No.	Accreditation Criteria	Pass	(Notes)
12.1(a)	When in receipt of a cargo for which a pre-alert has been received, the receiving site should confirm arrival of the goods and the status of the shipment to the originator as soon as practicable.		
12.1(b)	For truck shipments the collection site should pre-alert the destination site with predetermined information in an agreed format including as a minimum: departure time, expected arrival time, truck company, driver name, vehicle registration number, and trailer seal numbers.		This information should be passed at the time of departure of the vehicle. Where pre-alerts are not acknowledged the dispatcher should seek to contact the receiving person to ensure that the delivery can be made.

## Vetting and Recruitment

(Also see appendix 'A')

Main Doc Ref No.	Accreditation Criteria	Pass	(Notes)
14.1(a)	All employees must provide their employer with an appropriate criminal records check. New employees must also supply a 5 year checkable employment (unemployment) history.	M	This requirement must form part of the job application process. Unfortunately there is substantial evidence that many crimes in this industry are 'inside jobs.' It is important that all employees are appropriately vetted.
14.1(b)	All employment application forms should contain all the questions and all the declarations set in "Application for Employment (Suggested Format)" - Appendix 'A' to the AIMSS document.		