Operations Security & Counter Terrorism policy

General Statement

The modern world can feel like an increasingly dangerous place. The use of vehicles as a weapon to injure and kill people has become a real threat, which means people who operate and drive commercial vehicles need to act. It is vital that transport businesses like ours adopt a responsible approach to security. The agencies, which are charged with protecting all members of society, have identified some simple and inexpensive procedures to assist businesses like the A1 Group, Transport managers and drivers.

The guidance outlines the steps all our Drivers and employees can take to help keep the public and our business safe from attack.

This Policy covers:

- security culture – including pre-employment checks for staff and drivers
- site security – including vehicle access and operating centres
- vehicle security – including checking vehicles and what to do if a vehicle is taken

It also contains a top 10 list of actions for commercial vehicle drivers.

The A1 Group key message is for our business and its employees to take security as seriously as we take safety.

The business has nominated Clive Owen, Director as the Operations Security & Counter Terrorism champion.

Introduction

Purpose of this Guidance

This policy sets out straight forward steps that can help mitigate the threat of goods vehicles being used in vehicle as a weapon attack.

As well as helping to keep the public safe by deterring would be attackers from using your fleet, following this advice will:

- help prevent acts of terrorism
- help protect your organisation's reputation
- demonstrate your commitment to Corporate Social Responsibility
- help to improve security culture within your business
- help reduce crime

This policy covers security measures for:

- building and embedding a positive security culture and behaviours
- personnel security
- operating centres and maintenance facilities
- transport managers and drivers
- vehicles
- general security issues

This policy sets out the simple steps the A1 Group takes to promote a good security culture in the business and help keep drivers, sites and vehicles secure.

The security checklist provides advice for drivers, to reduce the risk of their vehicles being stolen for use in an attack.

Links to a wide range of more detailed official guidance.

Remember, good security = good business

What is a Goods Vehicle?
For this policy the term 'Goods Vehicle' applies to a vehicle designed to carry goods or materials rather than passengers, from a small van to a large lorry.

What is a Vehicle as A Weapon attack?
An A1 Group vehicle can be used as a weapon intentionally to injure and kill people. This is referred to as a 'vehicle as a weapon (VAW) attack'.

VAW is a low complexity methodology requiring little or no training. With a plentiful source of vehicles on UK roads, it is therefore within the capability of individuals to try and steal one and use it in an attack.

Crowded public spaces are targeted by this type of attack. There are a range of online terrorist and extremist materials aimed at inspiring terrorists to carry out VAW attacks and previous attacks have encouraged copycats, who now see VAW as a successful means to cause terror. Lorries and vans pose an increased risk if used in VAW attacks because of their size, profile and weight, all of which increase the potential impact.

This is a real threat: there have been numerous VAW attacks in the UK and around the world in recent years, killing and injuring hundreds of innocent people.

Consequently, VAW remains a likely attack methodology for the foreseeable future. Following this policy will help reduce the possibility of one of our vehicles being used as a weapon.

People, Security Culture & Behaviours
What is a security culture?
A strong security culture will help mitigate security risks, including VAW by promoting compliance with security measures, awareness and vigilance.

A security culture is 'a set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security'.

The benefits of an effective security culture are:

- a workforce that are more likely to be engaged with, and take responsibility for, security issues
- increased compliance with protective security measures, such as those set out in this guidance
- reduced risk of insider incidents
- awareness of the most relevant security threats
- employees are more likely to think and act in a security conscious manner

Security behaviours in your organisation

A strong security culture will promote positive security behaviours across the A1 Group. Using the Centre for the Protection of National Infrastructure (CPNI) 5Es framework (Educate, Enable, Shape the Environment, Encourage the Action and Evaluate the Impact) the A1 Group can embed and sustain security behaviours within our workforce.

The CPNI 'Embedding Security Behaviours: using the 5Es Framework' document provides guidance on how to implement the 5Es within the A1 Group.

Vigilance and reporting suspicious behaviour

In an emergency always ring 999. Security awareness, vigilance and reporting suspicious behaviour, increases the likelihood that people with hostile intentions will be detected or deterred.

A1 Group employee vigilance complements other elements of protective security. Procedures for reporting any unusual behaviour to supervisors and police, should be developed and briefed to all staff.

It is highly recommended reporting any concerns via the National Counter Terrorism Policing (NCTPHQ) Action Counters Terrorism (ACT) campaign:

'If you've seen or heard something that could suggest a terrorist threat to the UK do not ignore it, report it'.

Report suspicious activity to the police by calling confidentially on 0800 789 321 or through the report in confidence service on the page: https://act.campaign.gov.uk.

The public already contribute intelligence to around a third of the most serious terrorism investigations.

Staff should be reassured that they need not be concerned about wasting police time or getting someone into trouble.

Due to the nature of security operations, you may not hear back from the Police, this does not mean they have ignored your concerns.

Vigilance will be further promoted by putting in place systems for recording site security patrols, monitoring and checking visitors and vehicles.

Identification passes should be issued to staff and visitors and worn at all times. All staff should be encouraged to challenge anyone on your premises who is not wearing a pass.

A1 Group Security Plan

A security plan is the cornerstone of a secure goods vehicle operation that sets the basis for strong security behaviours, culture and security practice.

A company security plan should cover at least the following steps, themes and elements:

1. allocate security responsibilities to a staff member who has appropriate authority to make security related decisions and implement them
2. assess risks posed by your vehicle operations. Involve key business partners including customers, shippers, freight forwarders, carriers, security service providers, and insurance experts in the risk assessment, if possible. Define and understand the security risks in vehicle operations including the 'insider threat'
3. identify possible solutions that will prevent one of your vehicles being used in an attack, whilst considering options, for example, that all vehicles should be locked when not in use. Security plans and procedures should be updated regularly. Collect feedback from drivers and consider the drivers' needs and wishes in day-to-day vehicle security management. When implementing decisions ensure employees have been consulted. Undertake regular reviews to monitor results and progress
4. altogether, when designing security plans, managers should consider the five-step model illustrated above which guides them through the most important aspects and themes of goods vehicle security management

Countering the insider threat with pre-employment checks

An insider is a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

Insiders with access to the A1 Group processes and assets can be a source of threat. An insider could be a full time or part-time employee, a contractor or even a business partner. They could deliberately join our organisation to gain access to our organisation's assets to mount an attack, or they may be triggered to act at some point during their employment.

The A1 Group provides a trusted resource for staff to report security concerns or suspicions, either anonymously or otherwise, this is a positive way of nurturing a security culture within our business.

We conduct robust pre-employment checks for all employees and we believe this helps mitigate the insider threat by:

- deterring applicants who may wish to harm your organisation from applying for employment
- detecting individuals with an intent to harm your organisation at the recruitment/application phase
- and denying employment to individuals intending to harm your organisation, and deny employment in roles for which the applicant is unsuitable
-

Remember: deter - detect - deny

Consideration has been given by using **British Standard 7858 (or equivalent) for security screening of employees.**

This standard involves conducting basic identity, financial, employment and criminal records checks. We recommend that the following additional steps are taken when employing drivers:

- check a driver's references and previous employment history (minimum of five years)
- speak to previous employers
- inform applicants that false details on application forms may lead to dismissal
- check driving licences are valid and look for endorsements before you employ someone, and then at six-monthly intervals afterwards. All A1 Drivers are required to the business of any changes to their licence
- check if the applicant has any prosecutions pending or is waiting for sentencing by a court
- for agency drivers, the A1 Group ensures that the agency has carried out all of these checks including criminal records checks
- and use only reputable recruitment agencies that are affiliated with a recognised UK trade Organisation

Site Security

Secure sites prevent vehicles being stolen and potentially used in terrorist attacks

By having effective security measures at all A1 Group sites helps to create a controlled environment which will encourage positive security behaviours amongst staff, act as a deterrent and protect from theft and other criminal activity.

Organisations can consult their local Counter Terrorism Security Advisers (CTSAs) to agree a system for reporting and dealing with suspicious vehicle incidents, and liaise with them regarding securing their sites. CTSAs work with businesses and the community to identify and assess sites that may be vulnerable to terrorist or extremist attack. They also work with trade organisations and professional bodies to ensure counter terrorism protective security advice is incorporated into general crime prevention advice and guidance.

Basic security measures can help to ensure that an item is not concealed on board a vehicle when in Depot. Having clear signage in place can discourage unwanted access by vehicles and people.

Examples of site security measures:

- fit locks or tamper proof seals to lockers and equipment boxes;
- access to operating centres should be controlled with appropriate security arrangements i.e. fences, gates, security codes;
- vehicle keys should be stored in a secure locker with security codes. Keys should not be left in vehicles or on hooks in the office easily accessible to anyone

Visitors and contractors

All visitors and contractors accessing our premises are required to report to reception or an individual in authority to notify their arrival.

Visitors should sign-in, be issued visitor passes and have a legitimate reason for their visit. These identification passes should be worn and 'be visible' at all times, anyone not wearing a pass should be asked by a member of staff why they are not wearing a pass. Visitors should be escorted at all times when not in public areas.

This process provides audit information, including sign in/out times and the purpose of the visit, and can be crucial in the event of an emergency evacuation of the premises. Visitors and contractors should be given a security awareness briefing to include:

- where a pass is issued, it should be displayed prominently at all times while they are on the premises
- anyone without a pass or in an unauthorised area will be challenged
- if a vehicle has been parked on site, any work/parking permits should be displayed prominently in the
- windscreen
- remind them to be vigilant when on the premises and of what to do if they see a suspicious item or a person acting unusually
- all doors should be properly closed when leaving, particularly doors leading to non-public areas
- "Tailgating" into non-public areas should not be allowed
- worksites and equipment should be secured on leaving

Vehicle access at sites

The movement of any unauthorised vehicles on any A1 Group site should be strictly controlled If this is unavoidable, appropriate access controls are to be adopted for example: a parking permit system for staff, visitor and contractor vehicles or allowing pre-arranged deliveries only may be considered.

Security controls

All A1 Group sites with parked vehicles that are not in use are subject to security controls that include:

- physical access barriers around the site such as walls and fences which should be in good repair and maintained to acceptable standards
- access control measures at all entrances to prevent unauthorised access
- measures to protect vehicles on the site (locking of vehicles, regular patrols, or CCTV cameras to detect and monitor any unauthorised access)
- wherever possible vehicles, trailers and other material should not be parked/placed near or up against the fence, gates and walls as they may be used as climbing aids or cover from view from the CCTV cameras or guard force security patrols.

A1 Group sites

The movement of any un-authorised vehicles at operating centres should be prevented or strictly controlled with appropriate access control measures.

The A1 Group consult their local CTSA to agree a system for reporting and dealing with suspicious vehicles, and liaise with them regarding evacuation plans.

Security at Vehicle maintenance facilities

If A1 Group vehicles are required to be repaired and maintained off-site the business, ensures that the site's security is appropriate. Maintenance staff, including sub-contractors should be made aware of our company's vehicle security policies and procedures. Any maintenance agreement between the A1 Group and the vehicle maintenance company should include a duty to secure the vehicles and keys correctly.

CCTV

CCTV is central to most modern security systems.

Its primary purpose is to detect suspicious activity and act as a verification system for other security measures. CCTV can be a single or combination of systems and technologies to form the overall security solution.

The A1 Group use an electronic detection system assured by CPNI, It works on the five-minute rule. This assumes that each part of a perimeter or sensitive asset is viewed by either a guard or CCTV once every five minutes. This limits the potential time for an unauthorised activity and forces an attacker to act rapidly, making them more likely to trigger an electronic detection system.

Unsecure Locations

It is not always possible for vehicles to be parked in a secure location when on route.

An A1 Group driver is a lone worker and it is important they feel safe and secure whilst working.

If parking in an unsecure location, The A1 Group ensures that drivers satisfy themselves that the following checks are carried out:

- is the vehicle locked with windows closed? Do they have their keys on their person?
- have they activated the vehicles security devices where applicable?
- has anyone followed them, are they being watched?
- if possible, can they keep the vehicle in sight at all times?
- is the area well lit?
- when returning to their vehicle, does it look the same as when they left?
- are there any external factors that they could reasonably predict (e.g. weather) that could disrupt their route?
- does their company know where they are parking?
- are there parking areas recommended by others which they feel are safe and secure?
- **do not post your location on social media**
- if they are approached or stopped by police, or an authorised public body, only open the cab door window after officers have shown their identification and inform the A1 Group. If they suspect the individual is not an authorised officer, and they couldn't produce their warrant card, keep the cab locked and stay in the vehicle, drive to the nearest Police Station or call 999
- be mindful that the only public bodies with legal powers to stop you whilst driving are the Police, Driver Vehicle and Standards Agency (DVSA), Highways Authorities such as Highways England and those granted Community Safety Accreditation Scheme Powers (CSAS) powers by the Police.

If in any doubt, call the Police

Vehicle Security
Checking vehicles
Drivers should visually check their vehicle at the beginning and end of their journey.

Also, whenever they leave or return to their vehicle, they look for any signs that something has been concealed or the vehicle tampered with.

This can be included as part of the required roadworthiness 'walk around' check. A security check list for drivers supports this guidance.

Securing vehicles
Whenever vehicles are left unattended.

For example, at the start and end of a journey, during a comfort break or whilst parked as securely as possible, drivers ensure that all the doors and windows are closed, engine switched off and ignition keys are taken with them. For vehicles not requiring ignition keys, drivers ensure that they secure the vehicle appropriately before leaving (Annex A). Vehicles are not be left unattended with engines running.

Measures to prevent vehicles being taken by criminals or terrorists and used as a weapon include:

- vehicles should not be left unattended at the roadside with the engines running
- ignition keys should not be left in the vehicle whilst the driver is not present
- A1 Group vehicles that require the engine running, to operate auxiliary equipment when the driver is not in the cab, take appropriate measures to ensure against theft of the vehicle; this includes the provision of a second key to lock the cab doors
- alternative security measures are considered and used for vehicles not requiring an ignition key
- security measures are put in place at A1 Group Depots or other premises to prevent unauthorised access to vehicles
- A1 Group vehicles are be parked as securely as possible
- A1 Group Drivers are to report any concerns about unusual behaviour that occurs on or close to their vehicle

Vehicle Security Equipment

Security features that keep the driver and vehicle safe and secure should be considered during the vehicle procurement process.

In addition to the risk of vehicles being stolen for use in terrorist attacks, the additional costs to a business caused by the theft of a vehicle and/or load can be considerable.

The decision will depend on what type of operations are being undertaken. A vehicle being used to multidrop in a town centre are fitted with an ignition immobiliser, we also think about load space monitoring. However, the message is simple: if the Driver keeps the vehicle safe and secure and they reduce not only the costs to our business associated with economic crime, but they also deny a potential terrorist access to a large, heavy vehicle capable of causing great harm when driven deliberately into crowds of people.

The A1 Group regularly reviews what security and safety equipment is most appropriate for their vehicles, from sophisticated electronic engine immobilisers and in-cab cameras to simple steering locks: anything that deters the theft of the vehicle should be considered.

What to do if a vehicle

is taken If your vehicle is stolen call 999 and alert the call handler to the following information:

- circumstances of the vehicle being stolen.
- description of the vehicle including company name, registration details, aerial roof markings and any tracking software fitted in the vehicle.
- if you suspect that the vehicle has been stolen for a terrorist attack then make sure this is made clear to the call handler.

Drivers should also immediately alert the company who will have procedures in place for stolen vehicles.

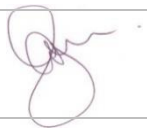
Disposal of vehicles
Prior to disposal or sale of vehicles to third parties.

All vehicles have their entire internal and external livery and other markings removed to avoid potential use by others for malicious purposes.

DfT contact details
Please contact DfT's Land Transport Security Division for further enquiries on goods vehicle security and VAW at: landsecurity@dft.gov.uk

Revision

The Company will make all employees aware of this Company Policy.

Signed: 	Date: 1/1/24

Stuart Cawthorne
Transport Manager

Next Review date 1st January 2025

Security tips for Goods Vehicle Drivers

1. Avoid talking about loads or routes with unauthorised persons (including over radios and telephones). Do not post information about your route or location on social media, be aware of your 'digital footprint', and take care to avoid unwitting disclosure of route/location through mobile phone security
1. settings and geolocation of pictures. Discuss high risk routes with the Transport Manager.
2. Lock and secure your vehicle whenever you leave the cab and keep the keys secure, including when
3. unloading and loading, always follow company security policies and instructions.
4. Carry out visual walk around checks when leaving and returning to the vehicle to make sure it has not been tampered with. Report any irregularity in loading, locking, sealing or documentation to your Company.
5. When conducting walk around checks, think Security as well as Safety.
6. Never carry goods for anyone, other than the authorised load.
7. If you are forced to change your route, inform the Transport Manager immediately.
8. If someone is acting suspiciously or something 'doesn't feel right' either at the depot or on the road, report it to ACT, call 0800 789 321 and contact your company.
9. Do not allow unauthorised passengers into the cab.
10. Keep your phone fully charged and on you at all times. Store important phone numbers.
11. Be mindful of your personal security. Keep ID documentation and wallets secure and out of sight.
12. Beware of attempts to deceive, such as by bogus Police and DVSA Officers - Stay vigilant always.

Glossary

ACT: Action Counters Terrorism, a national campaign by Counter Terrorism Policing to encourage the public to act on their instincts to help tackle the terrorist threat.

Cab: The cab is an enclosed space in a lorry where the driver is located.

Corporate Social Responsibility (CSR): CSR can help an organisation to show it is socially responsible and environmentally sustainable. To be considered as socially responsible, a company's activities should benefit society.

CPNI: Centre for the Protection of National Infrastructure, the Government authority that provides protective security advice to businesses and organisations across the national infrastructure.

CSAS: Community safety accreditation scheme powers, CSAS is a voluntary scheme under which Chief Constables can choose to accredit employed people already working in roles that contribute to maintaining and improving community safety with limited but targeted powers.

A1 Group Site: A base or depot for our Vehicles

Suspicious Behaviour: Any observed behaviour that could indicate terrorism or terrorism-related crime Transport Office/Operator/Supervisor: Management working in the company offices and are responsible for managing the execution, direction, and coordination of all transportation matters within the organisation.

Summary of sources and further information

Section	Topic	Organisation
Section 1: Introduction	CONTEST: The United Kingdom's Strategy for Countering Terrorism	HM Government
Section 2: Security Culture	Security Culture	CPNI
Section 2: Security Culture	ACT: Action Counters Terrorism	Counter Terrorism Policing
Section 2: Security Culture	Embedding Security Behaviours: using the 5Es	CPNI
Section 2: Security Culture	Optimising People in Security	CPNI
Section 2: Security Culture	Insider Threat	CPNI
Section 2: Security Culture	Personnel Security	CPNI
Section 2: Security Culture	Pre-employment Screening	CPNI
Section 2: Security Culture	British Standard for Security Screening Employees (BS7858)	BSI
Section 2: Security Culture	Pre-Employment Screening: Good Practise Guide	CPNI
Section 2: Security Culture	Crowded Places Guidance	NaCTSO
Section 3: Site Security	Working with counter terrorism security advisers	NaCTSO
Section 3: Site Security	Control Access	CPNI
Section 3: Site Security	Lone Working	HSE
Section 3: Site Security	Crowded Places Guidance	NaCTSO
Section 3: Site Security	CCTV Guidance	CPNI

Additional Sources of Information

Topic	Organisation
DfT Rental Vehicle Security Scheme (RVSS)	DfT
Dangerous Goods Security Training	DfT
Bus and Coach Security Recommended Best Practice Third edition	DfT
Fleet Operator Recognition Scheme	FORS
Earned Recognition Scheme	DVSA
Professional driving of lorries, buses and coaches	DVSA