ProtectUK

Section 3- Site security

ProtectUK publication date
10/12/2021

Effective security measures at operating centres and maintenance facilities can help 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.

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

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 onboard a vehicle when in maintenance centres. 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 the premises should be 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 site should be strictly controlled and ideally

prevented

If this is unavoidable, appropriate access controls should be adopted, for example, a parking permit system for staff, visitor and contractor vehicles or allowing pre-arranged deliveries only.

Security controls

All sites with parked vehicles that are not in use should be 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.

Operating centres

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

Transport Operators should 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 your vehicles are repaired and maintained off-site you should ensure that the site’s security is appropriate. Maintenance staff, including sub-contractors should be made aware of your company’s vehicle security policies and procedures. The maintenance agreement between the vehicle operator 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.

We recommend using an electronic detection system assured by NPSA, which can be sourced from the NPSA Catalogue of Security Equipment (CSE). Most of these work 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.

A driver is a lone worker and it is important they feel safe and secure while working.

If parking in an unsecure location, operators should ensure that drivers satisfy themselves that the following checks are carried out:

- is the vehicle locked with windows closed? Do you have your keys on your person?
- have you activated the vehicles security devices where applicable?
- has anyone followed you, are you being watched?
- if possible, can you keep the vehicle in sight at all times?
- is the area well lit?
- when returning to your vehicle, does it look the same as when you left?
- are there any external factors that you could reasonably predict (e.g. weather) that could disrupt your route?
- does your company know where you 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 you 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 your Transport Operator. If you 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 while 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

KEYWORDS
SITE
SECURITY CULTURE
VEHICLE AS A WEAPON
ACCESS CONTROL
THREAT