ANTI-TERRORISM AND INCIDENT PREVENTION

Main Author	Reviewer	Reviewer	Approver
Michel Mauricio	Liam O'Meara	Michael Carroll	Tom Barrett

REV	Date	Status / Description of Changes
Michel Mauricio	05/08/2019	Updating all laws/regulations dates to the current standard. Adjusting template, for a more clear layout.

Thomas Barrett – Director

Reviewed : 05/08/2019

RIP®

TERRORISM RISK AND INCIDENT PREVENTION

Policy and Procedures

preventterrorism.co.uk

This policy includes the company policy statement, procedures and associated documentation to ensure our staff are suitably aware and prepared to deal with the circumstances of extremist and terrorist action through increased awareness, security and vigilance.

Contents

Document reference: FS-011
Issue version: 0.1
Dated: 11 October 2017

1. Purpose

The purpose of the Terrorism Risk and Incident Prevention (TRIP) policy is to minimise this risk through promoting and raising awareness, security and vigilance, as well as ensuring our staff are prepared to deal with the extraordinary circumstances of terrorist, extremist and criminal acts.

2. Scope

This policy applies to all staff in our organisation. This includes Senior Management and all staff involved in security, transport operations, fleet management, training and all driving duties.

3. Policy statement

The UK faces a range of threats to its security and there is a serious and sustained risk from international and domestic terrorism. The threat level in the UK has been 'Severe' since 29th August 2014 (with spikes to 'Critical') which means there is a high likelihood of future terrorist attacks. Historically, the terrorist threatintheUKhasbeenfromdissidentRepublicanterroristgroupsconnectedtoNorthernIreland.More recently the terrorist threat in the UK has come extremist organisations such as Al Qaeda, ISIS, ISIL and National Action.

Although it is highly unlikely that our company would be a direct target of an organised attack from such terrorist networks, there have been recent terrorist attacks, and more significantly the attacks across Europe using commercial vehicles as a weapon. As such, we recognise our responsibilities and duty of care when protecting employees, our customers and the general public from the threat of terrorism.

This policy is not intended to cause undue fear, anxiety or alarm, but rather to raise and promote awareness amongst all employees of the need to be perceptive, proactive, prepared and vigilant. We should all understand our roles and responsibilities should a situation arise. Being prepared and having suitable procedures and responses in place is a proactive way to counter terrorism. Our actions alone may not prevent a terrorist attack but could help save lives and property as well as permitting the Company to continue to operate as usual. We will ensure that the following is in place;

a. Adequate training, information and equipment is provided to all staff, especially to those involved directly in security and the management and operation of vehicles.
b. Emergency response plans are in place that cover a wide range of possible security breaches and incidents.
c. Competent staff are appointed to deal with imminent risks and danger that may result in immediate action drills being undertaken.
d. Incidents involving breaches of security are managed safely and sensitively and are reported to the relevant authorities promptly.
e. An emergency and business continuity plan is in place to enable a simultaneous response to a security incident and a return to 'business as usual' as soon as possible.
f. The measures in place for countering terrorism are aligned to the measures in place help against other threats, such as theft and crime.

We are committed to a coordinated communication programme to ensure all staff are aware of the TRIP policy and its supporting procedures. The policy will be reviewed periodically considering the terrorist alert state to ensure it continues to be relevant and effective.

4. Protective security and managing the risks

To manage risks, we need to understand and identify the security threats and our vulnerability to those threats. The national terrorism threat levels that give an indication of the likelihood of a terrorist attack are listed at Appendix 1.

A threat is a malicious event, instigated by an individual or group, which has the potential to cause loss of or damage to an asset (people and property). Dealing with the threat of a security breach or terrorist attack, which might prejudice the safety of our staff, our customers or the general public or disrupt operational activity, is only a small part of our area of work. However, it is important to give it due consideration in security and emergency plans and procedures. This will help to decide:

a. What type of security and contingency plans we need to develop?
b. What security improvements we need to make taking account of cost and their impact on existing security measures?
c. What existing security measures should be routinely reviewed as well as compliance with these?
d. What level of staff communications and awareness training is required as well as practiced contingency arrangements?

Once an area of vulnerability has been identified we will apply appropriate protective security measures to reduce the risk to as low as reasonably practicable using the following risk assessment process. The full process is documented at Appendix 2:

Step 1	Step 2	Step 3	Step 4
Identify the threat	Identify the vulnerabilities	Implement and communicate security measures	Review security measures and security plans

5. Roles and responsibilities

5.1 Senior management must ensure that:

a. The TRIP Policy is published and it is effectively communicated to all staff across the organisation.

b. Operational management staff are resourced, trained and empowered to conduct the duties outlined in this policy.

c. That any related policies, such as theft and crime, and supporting procedures are consistent with this policy.

5.2 Operational management must ensure that:

a. They are conversant with all procedures and documentation outlined in this policy and that the policy is fully implemented.

b. All staff, and in particular drivers, are aware of their duties and responsibilities under this policy.

c. Any deviation from this policy is fully documented and justified for approval by Senior Management.

d. All incident evidence is collected and recorded to report to the emergency services and inform any post-incident investigation.

e. The in-house communications department is liaised with if there is a need to increase security awareness across the organisation.

f. Exception reports on any incidents are provided to Senior Management for immediate review.

5.3 All staff must ensure that they:

a. Are aware of their responsibilities under the TRIP policy.

b. Are aware of the current threats, vulnerabilities and their responsibilities in countering them.

c. Are vigilant at all times.

d. Report all suspicious occurrences and anything which may lead to a breach of security.

e. Report contact with any person which gives rise to suspicion.

f. Apply the procedures for minimising threat levels such as maintaining vehicle and site security.

g. Follow the actions to take in the event of a suspicious or threatening incident.

6. TRIP procedures

6.1 TRIP Risk Assessment procedure.

6.2 Vehicle security, theft prevention and hijack procedure.

6.3 Vehicle Borne Improvised Explosive Devices (VBIEDs).

6.4 Identifying suspicious people, suspicious activity.

6.5 Bomb threat procedure.

6.6 Actions to take in the event of discovering a suspect device.

6.7 Actions to be followed in the event of a direct attack.

7. Related policies and procedures

7.1 Personnel security policy.

7.2 Access control policy and vehicle security procedures.

7.3 Driving eligibility and transport control procedures.

7.4 Information security and business continuity policy.

7.5 Driving for work policy.

7.6 Fire safety policy.

7.7 Health and safety policy.

8. References

8.1 The Health and Safety at Work etc Act 1974
8.2 The Management of Health and Safety at Work Regulations 2006
8.3 CPNI Personnel Security: Managing the Risk
8.4 ACPO Expecting the Unexpected - Business continuity in an uncertain world

9. Appendices

Appendix 1 - Terrorism threat levels.
Appendix 2 - TRIP Risk Assessment: Protective security and managing the risks.
Appendix 3 - Communications and training.
Appendix 4 - Vehicle security, theft prevention and hijack procedure.
Appendix 5 - Vehicle Borne Improvised Explosive Devices.
Appendix 6 - Identifying suspicious people and suspicious activity.
Appendix 7 - Bomb threat procedure.
Appendix 8 - Bomb threat record card.
Appendix 9 - Actions in the event of a suspect device.
Appendix 10 - Actions in the event of a direct attack.

10. Document history

Version	Date	Change Summary	Author	Approved by

A1. Terrorism threat levels

Terrorism threat levels give an indication of the likelihood of a terrorist attack. They are based on a range of factors and indicators; including current intelligence, recent attacks and what is known about terrorist intentions and capabilities.

Threat level definitions

The national threat level is available on the Security Service, Home Office and UK Intelligence Community Websites. This is rated as follows:

a. Low – An attack is unlikely.
b. Moderate – An attack is possible but not likely.
c. Substantial – An attack is a strong possibility.
d. Severe – An attack is highly likely.
e. Critical – An attack is expected imminently.

Response levels

Our business Response Levels categorise the protective security measures that we should apply. They are informed by the threat level but also consider specific assessments of vulnerability and risk. There are a variety of site specific security measures that we can be applied within response levels.

The specific security measures deployed at different Response Levels should not be made public, to avoid informing anyone about what we know and what we are doing about it. The three Response Levels of are as follows:

Threat Level	Response Level	Definition
Critical	Exceptional	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk. This includes: • Targeted specific staff communications and awareness raising. • Maximum level of managerial checks made on security procedures.
Critical Severe and substantial	Heightened	Additional and sustainable protective security measures. This includes: • Increased specific staff communications and awareness raising. • Increased level of managerial checks made on security procedures.
Moderate and low	Normal	Routine baseline protective security measures. This includes: • Routine specific staff communications and awareness raising. • Routine level of managerial checks made on security procedures.

If the threat level changes, a site-specific TRIP Risk Assessment is to be carried out.

A2. TRIP Risk Assessment: Protective security and managing the risks

To manage risks, we need to understand and identify the security threats and our vulnerability to those threats. To help achieve this we follow a four-step risk assessment process.

Step 1 - Identify the threat

To counter terrorism we must understand terrorist intentions and capabilities. What they might do and how they might do it is crucial to assessing threat. In identifying the threat, the following questions should be considered:

a. Learn from the government and media about the current security climate, or about recent terrorist activities.
b. Know whether our depots, visitors, sponsors, contractors, occupiers or staff would particularly attract a terrorist attack.
c. Know whether our logistic operations for any organisation might attract a terrorist attack.
d. Could collateral damage occur from an attack on a high-risk neighbour?
e. Contact the local Police to inform us about crime and other problems in the area.
f. Know how our business and vehicle assets might be exploited to aid terrorist objectives.
g. How we will communicate information about the threat and how we should respond to all our staff.
h. Assess what policies and procedures are in place to respond to an attack that led to loss or disruption of business or transport assets.

Step 2 - Identify the vulnerabilities

Our priorities for protecting against vulnerabilities are categorised as follows:

a. People – Staff, customers and the general public.
b. Physical assets – Vehicles, equipment, buildings and contents.
c. Information – Plans, documents and electronic data.

We have procedures in place for dealing with fire, crime, employee background checks and protection from IT viruses and hackers.
Other areas of vulnerability include:

a. Information about our organisation that is publicly available through the inter net or in public documents.
b. Anything that identifies installations or services that are vital to the continuation of our business or the business of our customers.
c. Any dangerous substances or hazardous materials that may be attractive to terrorists.

Our measures should limit accessibility to people, physical assets and information and we should conduct stringent checks on the people we recruit or contract.

Step Three - Identify measures to reduce risk

The nature of our business of carrying valuable goods on the public highway, therefore makes us more likely to suffer from the effects of theft than from terrorism. Although the likelihood of a terrorist or criminal act on our operation may be low, the impact of such an act can be horrific.

Many of our security measures used to deter theft and other crimes are also effective against terrorist risk. Whatever additional security measures we consider, an integrated approach to security is essential. Any additional security or specific counter terrorism measures, should be cost-effective through forward planning. Measures should always be categorised as personnel, physical and information security.
They should consider that:

a. Existing security measures are reinforced to all staff to mitigate any bad habits that may have developed.
b. Reinstating existing security practices and regularly reviewing existing security policies and procedures will bring benefits.
c. There is little point investing in costly security measures if they can be easily undermined by a disaffected member of staff or a relaxed recruitment process.
d. The security of vehicle assets, equipment and their keys is paramount and effective controls must be in place.
e. The identified vulnerabilities and security measures are designed into any new processes, premises or buildings.

We must make it easy for staff to understand and accept the need for security measures and how to raise concerns or report observations. Security is a part of everyone's responsibility and not just for security management.

Step Four: Review security measures and security plans

We must adopt a method that measures the effectiveness our security procedures and compliance with them. This may include the revising our managerial checks and auditing regime to ensure that the TRIP policy is effective and enforced.

It is important to monitor and review the policy and its procedures to continuously improve as new vulnerabilities are identified. This includes monitoring changes in the business that may result in new threats. Security measures must be modified to minimise any new threats. Periodically, it is crucial to maintain the relevancy of the TRIP policy. New procedures may be added when necessary and obsolete policies may also be withdrawn.

Security training, rehearsals and exercises should be conducted. Coordinated rehearsals can be conducted with other partners such as, emergency services and local authorities. Live exercises should be considered to ensure that security measures remain accurate, workable and up-to-date.

A3. Raising TRIP awareness

Our communication strategy for raising awareness the terrorist threat among staff include the TRIP policy requirements and the supporting procedures for managers, operational staff and drivers.

How our staff behave is a key indicator of our security culture. Being vigilant and aware demonstrates that it is not just security guards and Close Circuit Television (CCTV) that hostile individuals need to worry about.

We will raise awareness through our routine communications and run an ongoing vigilance behaviour campaign. In support of our TRIP policy we will use the staff handbook, toolbox talks, workplace posters, wallet cards to embed a culture of vigilance.

The TRIP campaign will be supported by specific training for managers, operational staff and drivers.

TRIP Training for Managers and Supervisors

Managers and Supervisors need to understand the importance of Terrorist Risk and Incident Prevention (TRIP). All Managers and Supervisors will attend the half day TRIP workshop to ensure they have the knowledge, skills and attitude to instil a culture of vigilance across our operation.

This workshop covers the following:

Understanding the issues relating to the threat from terrorist actions and criminal activity within Logistics Operations by outlining the following; the nature/type of threat, the current threat levels and what they mean.

Clarifying suggested 'best practise' and recognising how by having effective policies and procedures in place will protect the business. Policies and procedures would include guidance within the Driver's handbook and during Induction training.

Suggested preventative measures to enhance the company approach in the following areas; Driver safety, vehicle and loads security, safeguarding of vehicle keys, signing for keys. The roles and responsibilities of the driver concerning the walk around check, security of the vehicle running whilst unattended, route planning, considerations and routine stops. Raising general awareness of drivers to prevent criminal activity, vehicle and load theft and High Value goods from potential terrorist factions and criminal groups.

Clarifying how and who to report an incident to; including, the nature of the information required / needed by the security services as well as providing guidance information for drivers and operators, as well as accessing further information and resources that are available that may enhance Transport Operations safety and security.

TRIP Training for commercial fleet drivers

Our commercial drivers need to understand the terrorist threat and criminal activity to be able to react accordingly. All commercial drivers will attend the TRIP Driver CPC course to ensure they have the knowledge and skills to be vigilant and the confidence to deal with suspicious or threatening acts.

The training objectives for this course are;

- Provide HGV drivers with the underpinning knowledge and understanding relating to the background, activity and methods adopted by International and Domestic terrorists that concern all who operate within the Transport Industry.

- By identifying and describing the types of risks and threats will enhance the driver and employer roles and responsibilities when carrying out their tasks and duties.

- Outlining preventative and safe guarding measures that could be adopted by the Transport Industry to protect their employees and the general public.

- Explain and provide an understanding to delegates of the control measures and methods that could be followed as a result of a terrorist incident or attack using a vehicle as a weapon.

A4. Vehicle security, theft prevention and hijack procedure

Road freight theft costs the UK economy £250m per year. On average there are 1,400 incidents of theft of road freight vehicles and engineering plant per year alongside 2,700 reported thefts from HGVs. National theft hotspots include the A1, A19, A34 and A40.

More significantly commercial vehicles are being used as a weapon in terrorist attacks with target areas being densely populated city areas.

Preventative security measures

To help deter a theft or hijacking and the opportunistic incident, drivers must follow preventative security measures:

a. Safety and security of vehicle:
   1) Always keep keys with you.
   2) Do not leave keys in the vehicle, in the ignition or unattended.
   3) Always lock your cab and your vehicle when you are either working away from the vehicle, or on the back of the vehicle.

b. Stopping for breaks and rest – Always consider:
   1) Parking your vehicle off the street where possible.
   2) Parking your vehicle legally in secure, well-lit areas.
   3) Using an authorised lorry park if possible.
   4) Not parking at the roadside in isolated areas.
   5) Is it legal to park there?
   6) Does it look safe?
   7) Are other vehicles parked up, if not why not?
   8) Are there security lights, fencing, gates or CCTV?
   9) Can you get a mobile phone signal?

c. Preventing hijacks – Although hijacking is rare always consider:
   1) Never pick up un-authorised passengers or hitch-hikers.
   2) If you are collecting a co-driver, know who you are picking up.
   3) Verify unknown personnel. They may be wearing our company logo or uniform but it does not mean that they are working for us.
   4) Questioning the identity of anyone suspicious.
   5) Avoid having a set pattern or routine.

Heightened preventative security measures

The following preventative security measures should be considered to counter the probability and severity of Improvised Explosive Devices (IEDs) at:
Normal threat level: For business as usual, we will exercise effective site access controls for vehicles and identity the driver of delivery vehicles, contract vehicles and any passengers.

Heightened and exceptional threat levels: We will establish the TRIP vehicle check regime (see Appendix 5) and incorporate this into the routine driver walkaround checks. Physical barriers to keep unauthorised vehicles at a safe distance will be considered where appropriate.

A5. Vehicle Borne Improvised Explosive Devices

Vehicle Borne Improvised Explosive Devices (VBIEDs) are one of the most effective weapons used by terrorists. They can deliver a large quantity of explosives to a target, precisely, timely and with catastrophic effect. They can be detonated from a safe distance using a timer or remote control, or can be detonated on the spot by a suicide bomber.

Types of VBIED attack

Terrorists using VBIEDs, generally select targets where they can cause most damage, inflict mass casualties or attract widespread publicity. There are five main attack types that may use a VBIED:

a. Parked: A hostile vehicle armed with a device parked close to terrorist target.
b. Encroachment: A hostile vehicle armed with a device exploits gaps in the site perimeter or tailgate a legitimate vehicle through a site access point.
c. Penetrative: A hostile vehicle armed with a device may be used to breach a building or physical perimeter resulting in device detonation.
d. Deception: A hostile vehicle armed with a device may be modified to replicate a legitimate vehicle and used to gain site access.
e. Duress: A member of staff could be forced to open a site access point or forced to take a device in their vehicle to a vulnerable location.

Preventative security measures

TRIP vehicle check regime - When the threat Response Level is at either heighted or exceptional, additional security checks should be conducted in addition to the routine vehicle walk around checks to look for anything suspicious.

The TRIP walk around check helps identify anything suspicious. The most likely place to find a VBIED if the vehicle has been locked is underneath the vehicle.

Before touching the vehicle, conduct the following external checks:

a. Dirt on the ground that may have been dislodged.
b. Loose wires or strands of wire or tape.
c. Marks on the ground, such as footprints, jack or jack stand impressions.
d. Signs of forced entry around doors, windows, bonnet, and load area.
e. Fingerprints and smudges on the cab and load area doors.
f. The exhaust pipe for any implanted objects.
g. Fuel cap for tampering.
h. Wheel arch and tyres.
i. Under the front grill / bonnet.
j. Around the fifth wheel.
k. In the chassis.
l. On the load bed.
m. In storage compartments or tool bins.
n. In and around ancillary equipment.

Check inside the vehicle:

a. Under the cab seats and dashboard.
b. On the floor for packages partially hidden under the front seat.

If you suspect anything suspicious:

a. Do not touch or tamper with any suspect device.
b. Do not attempt to move vehicle.
c. Move away to a safe distance and find cover.
d. Try and keep other people away from the vehicle.
e. Do not use a mobile phone in the immediate vicinity.
f. Call 999 or the Police anti-terrorist hotline on 0800 789 321 to report an immediate threat to life or property.

A6. Identifying suspicious people

You cannot identify terrorists or criminals by neither their religion nor their creed or colour.
Too many of us stereotype terrorists and criminals where one cannot determine if someone is a terrorist or criminal just by their appearance.

Terrorists and criminals come in different forms and assuming someone is a terrorist or a criminal could prove to be inaccurate and may well cause offence to different ethnic groups or people from different backgrounds or social groups.

Many bomb attacks are preceded by reconnaissance or trial runs. Hostile reconnaissance is used by people who provide information to terrorist organisations on potential targets.

The aim of hostile reconnaissance is to obtain a profile of a target location, determine the best method of attack and determine the optimum time to conduct an attack. Reconnaissance operators may visit potential targets many times prior to the attack.

Hostile reconnaissance operators

Vigilance and good preventative security help recognise those engaged in hostile reconnaissance, disrupt a planned attack and produce important intelligence leads. You must report a suspect reconnaissance operator if anyone is:

a. Taking significant interest being taken in the outside site buildings including parking areas, delivery gates, doors and entrances.
b. Taking significant interest in the location of CCTV cameras and controlled areas.
c. Asking unusual questions, such as, security and evacuation measures, staff routines or social places.
d. Parking, standing in the same area on numerous occasions with no reasonable explanation.
e. Taking pictures, filming, making notes, sketching security measures count or counting pedestrians/vehicles.
f. Conducting overt or covert photography.
g. In possession of photographs, maps, blueprints etc, of critical infrastructures, electricity transformers, gas pipelines, etc.

Reconnaissance operators may conduct prolonged static surveillance disguised as demonstrators, street sweepers, or stopping to have 'car trouble.'

Suspicious events

Unusual activities that must be treated as suspicious and reported includes:

a. Anyone attempting to access unauthorised areas.
b. Attempts to disguise identity - motorcycle helmets, hoodies, etc.
c. Vehicles looking out of place.
d. Erratic driving.
e. Vehicles appearing overweight.
f. Vehicles and packages left unattended.
g. Delivery or contractor vehicles arriving at wrong or outside routine times.
h. Vehicles emitting suspicious odours e.g. fuel or gas.
i. Recent damage to perimeter security, breaches in fence lines or walls.

Suicide bombers

The use of suicide bombers is a very effective method of delivering an explosive device to a specific location. Suicide bombers may use a HGV, vans or other kind of vehicle as a bomb or may carry or conceal explosives on their person.

Both kinds of attack are generally perpetrated without warning. The most likely targets are mass casualty crowded places, symbolic locations and key installations.

There is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the Police.

If you suspect a suicide bomber follow the Run – Tell – Hide protocol outlined at Appendix 10 - Immediate actions in the event of a direct attack procedure.

Can I help you?

If someone appears out of place or is acting differently, an appearance of vigilance can put them off. Enquiring "Can I help you?" is a simple tactic to raise the profile of your vigilance.

If you suspect anyone or anything suspicious:

a. Do not spread information about your suspicion to avoid panic.
b. Do not try to overpower suspects.
c. Observe discretely and record the event for evidence purposes.
d. Try to remember as many details about appearance and behaviour.
e. Report to security management for CCTV monitoring.
f. Call 999 or the Police anti-terrorist hotline on 0800 789 321 if there is an immediate threat to life or property.

A7. Bomb threat procedure

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist.

If a bomb threat is received by phone:

a. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
b. Listen carefully, be polite and show interest.
c. Try to keep the caller talking to learn more information.
d. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
e. If your phone has a display, copy the number and/or letters on the window display.
f. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember and try to get exact words.
g. Immediately upon termination of the call, do not hang up, but from a different phone, contact management or security immediately with your information and await further instructions.

If a bomb threat is received in writing:

a. Handle any notes as minimally as possible.
b. Do not delete any email messages.
c. Contact management or security immediately and await further instructions.

Identifying suspicious packages

Signs of a suspicious packages include:

- No return address.
- Poorly handwritten.
- Excessive postage.
- Misspelled words.
- Stains.
- Incorrect titles.
- Strange odour.
- Foreign postage.
- Strange sounds.
- Unexpected delivery.

If a suspicious package is identified:

a. Do not use two-way radios or mobile phones; radio signals have the potential to detonate a bomb.
b. Do not activate the fire alarm.
c. Do not touch or move a suspicious package.
d. Call 999 or the Police anti-terrorist hotline on 0800 789 321 to report an immediate threat to life or property.

A8. Bomb Threat Record Card

Date:	
Time of Call:	
Time caller hung up:	

Ask the caller:

Where is the device located?	
When will it go off?	
What does it look like?	
What kind of device is it?	
What will make it explode?	
Did you place the device?	Yes/No
Why did you place the device?	
What is your name?	

Exact words of the threat

Male or Female?	
Approximate age	
Where is the caller location? (background noise)	
Is voice familiar? If so, who does it sound like?	

Information about caller

Caller's voice

- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Clear
- ☐ Clearing throat
- ☐ Coughing
- ☐ Cracking voice
- ☐ Crying
- ☐ Deep breathing
- ☐ Disguised
- ☐ Laughter
- ☐ Lisp
- ☐ Local
- ☐ Loud
- ☐ Nasal
- ☐ Normal
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Slurred
- ☐ Soft
- ☐ Stutter

Background sounds

- ☐ Animal Noises
- ☐ Booth
- ☐ Conversation
- ☐ Factory machinery
- ☐ House Noises
- ☐ Kitchen Noises
- ☐ Motor
- ☐ Music
- ☐ Office machinery
- ☐ PA system
- ☐ Street Noise

Threat language

- ☐ Incoherent
- ☐ Irrational
- ☐ Message read
- ☐ Profane
- ☐ Taped
- ☐ Well-spoken

If you receive a bomb threat

Call 999 or the Police anti-terrorist hotline on **0800 789 321** to report an immediate threat to life or property.

A9. Actions in the event of a suspect device

In the event of a suspect device there may be little time to think about what actions need to be taken. It can be stressful and tense moment. No one should feel embarrassed if they think something is suspicious, no should think somebody else will report it.

Immediate actions: Suspicious items or suspect devices

When dealing with suspicious items apply the "4 C's" protocol:

Confirm - whether or not the item exhibits recognisably suspicious characteristics. The **HOT** protocol may be used to inform your judgement:

a. Is it **HIDDEN**? Has the item been deliberately concealed or is it obviously hidden from view?
b. **OBVIOUSLY** suspicious? Does it have wires, circuit boards, batteries, tape, liquids or putty-like substances visible? Do you think the item poses an immediate threat to life?
c. **TYPICAL** Is the item typical of what you would expect to find in this location?

Do not touch the item and ask if anyone has left it.

Clear the immediate area - Take charge and move people away to a safe distance:

a. Move at least 100m away, even for small items.
b. Keep yourself and other people out of line of sight of the item.
c. If you cannot see the item then you are better protected from it
d. Take cover, think about what you can hide behind. Pick something substantial and keep away from glass such as windows and skylights.
e. Cordon off the area.

Control access to the cordoned area

a. Members of the public should not be able to approach the area until it is deemed safe.
b. Try and keep eyewitnesses on hand so they can tell Police what they saw.

Communicate but do not use mobile phones or radios within 15 metres

c. Call **999** or the Police anti-terrorist hotline on **0800 789 321** to report an immediate threat to life or property.

A10. Actions in the event of a direct attack

Direct terrorist attacks using firearms, bombs and vehicles are infrequent.
However, it is still important to consider this method of attack and a proportionate response to cope with such an incident. Dependent on the attack type determines the responding security measures required.

More significantly commercial vehicles are being used as a weapon in terrorist attacks with target areas being densely populated city areas.

ETHANE - Initial actions at a terrorist major incident

a. **E**xact location.
   1) Confirm nearest junction or exact address.
   2) Geographic size of the incident.
b. **T**ype of incident.
   1) Explosion, building collapse, firearms incident etc.
c. **H**azards.
   1) Identify the hazards present or suspected (such as number of hostiles, types of weapons etc.)
   2) Consider potential or secondary devices.
   3) Is evacuation necessary and safe?
d. **A**ccess routes
   1) Update with routes that are safe to use and clarify routes which are blocked.
   2) Nominate and search the Rendezvous Point (RVP).
e. **N**umber of casualties.
   1) List type and severity.
   2) Approximate number of dead, injured, survivors and witnesses.
f. **E**mergency services.
   1) List those Services present and those required.
   2) Conduct a joint dynamic hazard assessment with the emergency services.

Immediate actions: Firearms and weapons attacks

Run: To a place of safety. This is a better option than surrender or negotiating.

Your priority action is to remove yourself and any others from close proximity of the threat. Your ability to safely escape and your available options will be determined by proximity of the offender(s). Under firearm attack:

a. Take cover from gunfire, use:
   1) Brickwork or concrete walls.
   2) Vehicles (engine block area).
   3) Large trees and fixed objects.
   4) Earth banks/hills/mounds.
b. Conceal from view, in addition to the 'cover' options use:
   1) Building walls and partitions.
   2) Fences and other large structures.
   3) Blinds/curtains.
c. Try to confirm a safe escape route.
d. Attempt to leave the area as soon as possible if safe to do so.
e. Leave most of your belongings behind (keep your mobile phone).
f. Do not congregate in open areas or at evacuation or assembly points.
g. Provide guidance to people that might be unfamiliar with the area.

Hide: If there is nowhere to go. It is far better to hide than to confront. Remember to turn your phone to silent and turn off vibrate. Barricade yourself in if you can.

If you do not believe you can safely evacuate, or this may not be the best option, then you may need to consider sheltering in place, (providing there is a suitable option available).

a. Avoid congregating in open areas, such as corridors and foyers.
b. Consider locking or barricading yourself and others in secure areas.
c. Secure your immediate environment and other vulnerable areas.
d. Move away doors, remain quiet and stay there until told otherwise by appropriate authorities, or you need to move for safety reasons.
e. Silence mobile phones and other devices that may identify you.
f. Choose a location which may enable access to a more secure area.
g. Constantly re-assess the situation and your options based on the best available information.
h. Consider whether a safe escape route might now be possible if the circumstances change.
i. As a last resort, consider options for arming yourself with improvised weapons to defend yourself in the event that you are targeted.

Tell: The Police by calling 999 but only when it is safe to do so.

Call 999 or the Police anti-terrorist hotline on 0800 789 321to advise of your location and the situation. The more information you can pass on to Police the better, but never risk your own safety or that of others to gain it. If it is safe to do so, obtain the following information:

a. Exact location of the incident.
b. Description of the attacker and if they are taking a specific route.
c. Details of any weapons or vehicles being used.
d. Number of people in the area and any that have been injured.
e. The motive or intent of the offender (if known or apparent).

You may be asked to remain on the line and provide any other information or updates that the operator requests or if the situation changes.

Consider providing information and advice to others that may be in your area that may be unsure of the current location of the threat and what they should do.

Police response

In an attack involving firearms a Police officer's priority is to protect lives. One of their priority actions to achieve this will be to locate the offender and effectively manage that threat as quickly as possible, which could mean initially moving past people who need help. As more Police resources become involved they will attempt to quickly provide support and guidance to persons affected by the incident. At some stage they will generally conduct a 'clearance' search of the location to ensure that all persons involved or impacted by the incident are located, and to make the scene safe. Remember:

a. Police officers may not be able to distinguish you from an attacker.
b. Police officers may be armed and could point guns in your direction.
c. Avoid quick movements or shouting and keep your hands in view.
d. Police officers may initially move past you in search of the attacker.
e. Police officers may enter your location at some stage to secure the building and locate people that have hidden from the threat.
f. Promptly follow any instructions given by emergency responders.

Terrorism Risk and Incident Prevention (TRIP)
Delivered by Fleet Source

Established in 2012, Fleet Source was developed as a concept to deliver a service that at the time wasn't available in the sector: products and training that were simple, quality, effective and could be applied to any road transport fleet.

Since conception, we now provide driver and manager training for some of the UK's largest fleet operators in varied industries.

In February 2015, we partnered with AECOM and the Chartered Institute of Logistics and Transport (CILT) in the collectively named, FORS Community Partnership. It is our role within the Partnership to deliver the accreditation audits and approved training for the Scheme nationwide.
We are proud to have some strong credentials to our name which with determination, have made us one of the largest and most-trusted fleet training companies in the UK.

- We have the largest fleet compliance auditing team in the UK
- We are one of the top 10 JAUPT Centres in the UK
- We are the largest vulnerable road user training provider in the UK
- We are Transport for London (TFL's) primary contractor for their driver training programme.
- We deliver training in over 80 locations across the UK
- We employ over 50 trainers and over 70 auditors.
- We are part of the FORS Community Partnership alongside the Chartered Institute of Logistics and Transport (CILT) and AECOM
- Variety of courses developed in-house by a team of experienced and dedicated fleet training experts.

Some examples of the CPC training we can offer are:

- Safe Urban Driving/Van Smart
- LoCITY Driving
- TRIP (Terrorism Risk and Incident Prevention)
- TruckSmart
- Work Related Road Risk
- Safe, Green & Efficient, 11 CPC Modules
- Staying Legal

We also offer a range of Manager training including:

- In Vehicle Assessor
- TRIP (Terrorism Risk and Incident Prevention)
- In Vehicle Training
- Behavioural Aspects of Driving
- OLAT (Operator's Licence Awareness Training)
- Transport Management System Internal Auditors Course (TMS)
- Work Related Road Risk Managers Course
- FORS Practitioner Workshops
- CPC Manager Training

For further information, please visit fleetsource.co.uk or call 0345 600 4045

RIP®

TERRORISM RISK AND INCIDENT PREVENTION

Fleet source®

BETTER DRIVERS, BETTER BUSINESS

Fleet Source, Business Centre East, Fifth Avenue, Letchworth Garden City, Hertfordshire, SG6 2TS tel: 0345 600 4045