NPR MANAGEMENT SERVICES LTD T/A

SELECT SECURITY SERVICES

Counter Terrorism Procedures

CONTENTS

1. **Defeating Terrorism**

COMMUNITIES CAN DEFEAT TERRORISM

YOU CAN HELP MAKE YOUR COMMUNITY A HOSTILE PLACE FOR TERRORISTS

TERRORISTS NEED RECRUITS

Do you know anyone whose behaviour has changed suddenly?

TERRORISTS NEED STORAGE AND PLACES TO LIVE

Are you suspicious of a property where there is unusual activity that doesn't fit normal day-to-day life?

TERRORISTS NEED TRANSPORT

They need to move people and equipment around.

Has a vehicle sale or rental made you suspicious?

TERRORISTS NEED TO PREPARE

Are you suspicious of anyone taking photos of security measures such as CCTV cameras?

Let the police decide if the information you have is important.

2. Anti-terrorism Hotline

"You may feel it's probably nothing, but unless you trust your instincts and tell us we won't be able to judge whether the information you have is important or not.

Remember, no piece of information is considered too small or insignificant.

Our specially trained officers would rather take lots of calls which are made in good faith, but have innocent explanations – rather than not getting any at all.

We want you to look out for the unusual – some activity or behavior which strikes you as not quite right and out of place in your normal day to day lives.

It's probably nothing but… if you see or hear anything that could be terrorist-related trust your instincts and call the Anti-Terrorist Hotline on 0800 789 321."

Reporting suspicious activity to police that does not require an immediate response, contact the **ANTI-TERRORIST HOTLINE – 0800 789 321**

Any incidents that require an immediate response - **Dial 999**

3. Threat levels

Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities.

Critical	An attack is expected imminently
Severe	An attack is highly likely
Substantial	An attack is a strong possibility
Moderate	An attack is possible but not likely
Low	An attack is unlikely

The UK Government's Counter Terrorism Strategy aims to reduce the risk from International Terrorism, so that people can go about their business freely and with confidence. While the current terrorist threat presents many challenges, public safety is the absolute priority. The Government can never guarantee that attacks will not happen in the future, but its security effort is dedicated to reducing the risk as much as possible. Assessments of the level and nature of the threat from international terrorism are made by the Joint Terrorism Analysis Centre.

The Security Controller (i.e.: Building Manager, Security Manager, Supervisor or lead officer) is to ensure the correct threat level is prominently displayed.

Security Response Levels

The Response levels table is to be used as a guide line of the level of security measures that should be applied at any particular time. They are informed by the threat level but also take into account specific assessments of vulnerability and risk at local level.

Threat Levels	Response level	Response
Critical	Exceptional	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk
Severe Substantial	Heightened	Additional and sustainable protective security measures reflecting the broad nature of the threat combined with Specific business and geographical vulnerabilities and judgements on acceptable risk.
Moderate Low	Normal	Routine baseline protective security measures, appropriate to your business and location.

The Security Controller is to check the threat level regularly. This is done by visiting the MI5 website https://www.mi5.gov.uk/home.html. The threat level and response is also to form part of any security handover brief on a daily basis.

4. Hostile reconnaissance

Hostile reconnaissance is used by terrorists to provide information to operational planners on potential targets during the preparatory and operational phases of terrorist operations. Reconnaissance operatives may visit potential targets a number of times prior to the attack. Where pro-active security measures are in place, particular attention is paid to any variations in security patterns and the flow of people in and out.

The primary role of reconnaissance is:

• obtain a profile of the target location

• determine the best method of attack

• determine the optimum time to conduct the attack.

What to look for when trying to spot Hostile reconnaissance:

• Significant interest being taken in the outside of your premises including parking areas, delivery gates, doors, entrances and queues.

• Groups or individuals taking significant interest in the location of CCTV cameras and controlled areas

• People taking pictures – filming – making notes – sketching of the security measures in and around your premises. Tourists should not necessarily be taken as such and should be treated sensitively, but with caution

• Overt/covert photography, video cameras, possession of photographs, maps, blueprints etc. of critical infrastructures, electricity transformers, gas pipelines, telephone cables etc.

• Possession of maps, global positioning systems, (GPS), photographic equipment, (cameras, zoom lenses, camcorders). GPS will assist in the positioning and correct guidance of weapons such as mortars and Rocket Propelled Grenades (RPGs). This should be considered a possibility up to one kilometre from any target

• Vehicles parked outside buildings of other facilities, with one or more people remaining in the vehicle, for longer than would be considered usual

• Parking, standing or loitering in the same area on numerous occasions with no apparent reasonable explanation

• Prolonged static surveillance using operatives disguised as demonstrators, street sweepers, etc. or stopping and pretending to have car trouble to test response time for emergency services, car recovery companies, (AA, RAC etc.) or local staff

• Simple observation such as staring or quickly looking away

• Activity inconsistent with the nature of the building

• noted pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures, (bomb threats, leaving hoax devices or packages)

• The same vehicle and different individuals or the same individuals in a different vehicle returning to a location(s)

• The same or similar individuals returning to carry out the same activity to establish the optimum time to conduct the operation

• Unusual activity by contractor's vehicles

• Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or assault equipment, i.e. ropes, ladders, food etc. Regular perimeter patrols should be instigated months in advance of a high profile event to ensure this is not happening

• Attempts to disguise identity – motorcycle helmets, hoodies etc., or multiple sets of clothing to change appearance

• Constant use of different paths, and/or access routes across a site. 'Learning the route' or foot surveillance involving a number of people who seem individual but are working together

• Multiple identification documents – suspicious, counterfeit, altered documents etc.

• Non co-operation with police or security personnel

• Those engaged in reconnaissance will often attempt to enter premises to assess the internal layout and in doing so will alter their appearance and provide cover stories

• In the past reconnaissance operatives have drawn attention to themselves by asking peculiar and in depth questions of employees or others more familiar with the environment

• Sightings of suspicious activity should be passed immediately to the premises management for CCTV monitoring and the event recorded for evidential purposes.

In the event that you suspect that Hostile recognisance is taking place, the officer is to take the following steps.

1. Contact the Security Controller and report the suspicious persons/vehicle. Give as much detail as possible. Description, location vehicle etc.
2. Activate the body camera and approach the suspicious persons and engage in casual conversation.
3. After engaging with the suspicious person, monitor the individual from a distance and give the Security Controller regular updates of any potential movement.
4. Once the suspicious person has left site, an incident report is to be completed.

In the event that a patrolling officer reports suspicious behaviour, the Security Controller is to take the following steps:

1. Monitor the individual with the nearest CCTV camera if available.
2. Ensure all details reported by the officer are recorded in the D.O.B.
3. Report the incident to the anti –terrorism hotline **0800 789 321**
4. A CCTV review incident report is to be completed by the Security Controller if the suspicious person is caught on camera.
5. A snap shot is to be taken of the suspect and included in the security briefings to ensure all staff are aware if the suspect returns.

5. Firearms Attacks

Attacks involving firearms and weapons are still infrequent but it is important to be prepared to cope with such an incident. In the event of a Firearm attack NaCTSO **(National Counter Terrorism Security Office)** recommends the following four actions:

Stay Safe

- Under immediate gun fire, Take cover initially, but leave the area as soon as possible if safe to do so.
- Nearby gun fire, -Leave the area immediately, if possible and it is safe to do so.
- Leave your belongings behind.
- Do not congregate at evacuation points.

Cover from Gunfire	Cover From View
Substantial brickwork or concrete internal partition walls	internal partition walls
Substantial brickwork or concrete internal partition walls	Car doors
Engine blocks of motor vehicles	Wooden fences
Earth banks/hills/mounds	Curtains

If you can't escape, consider locking yourself and others in a room or cupboard. Barricade the door then stay away from it. If possible choose a room where escape or further movement is possible. Silence any sources of noise, such as mobile phones, that may give away your presence.

See

The more information that you can pass to police the better but never risk your own safety or that of others to gain it. Consider using CCTV and other remote methods where possible to reduce the risk. If it is safe to do so, think about the following:

• Is it a firearms / weapons incident? • Exact location of the incident.

• What else are they carrying? • Number and description of gunmen.

• Moving in any particular direction? • Type of firearm -long-barrelled or handgun.

• Are they communicating with others? • Number of casualties / people in the area.

Tell

• POLICE - contact them immediately by dialling 999 or via your Security Controller, giving them the information shown under 'See'.

• Use all the channels of communication available to you to inform staff, visitors, neighbouring premises, etc. of the danger.

Act

• Secure your immediate environment and other vulnerable areas.

• Keep people out of public areas, such as corridors and foyers.

• Move away from the door and remain quiet until told otherwise by appropriate Authorities or if you need to move for safety reasons, such as a building fire.

Please note that In the event of an attack involving firearms or weapons, an armed Police Officer's priority is to protect and save lives. Please remember:

• Initially they may not be able to distinguish you from the gunmen.

• Officers may be armed and may point guns at you.

• They may have to treat the public firmly. Follow their instructions; keep hands in the air and in view.

• Avoid quick movement towards the officers and pointing, screaming or shouting.

6. Suspect packages

In the event that an officer discovers a suspect package whilst on patrol, the following steps are to be taken:

- Do not touch suspicious items, report the item to the Security Controller.
- Use hand-held radios or mobile phones away from the immediate vicinity of a suspect item. Where possible use a landline telephone to communicate.
- Provide the Security Controller with a description (colour, size etc.) and the location of the package, time it was found, who found the package
- Utilise crowd barriers and cordon off the area of the suspect package to prevent others approaching the package.
- Prepare a brief to hand over to the police, this should include:
  WHAT is it? (Parcel, box, bag etc.)
  WHERE is it? (Are there access routes, obstructions etc.)
  WHEN it was found and if it has been moved since finding?
  WHY is it suspicious, reasons you are worried about it
  WHO the witnesses are?

Please note under no circumstances are officers to touch/open or move the suspect package.

In the event an officer reports a suspect package, the Security Controller is to take the following steps:

- Get a description, (colour, size etc.) and the location of the package time it was found, who found the package and immediately notify the police by calling 999.
- Deploy an officer / colleague to cordon off the area of the suspect package.
- Notify all capital properties management and security management immediately
- Monitor the area via CCTV and ensure no members of the public approach the cordoned off area.

- Keep all radio traffic to a minimum
- Record all occurrences in the D.O.B.

When a suspect package is found the area to be cordoned off is as follows:

Size of package	Area to be cordoned off
Small items	100 Metres
Medium Items	200 Metres
Large items/Vehicles	400 Meters

In the event that Security has been alerted to the possibility of a suspicious letter/package on site, all Officers should beware of the following information:-

Postal/letter bombs can come in any shape or size – parcels, envelopes or padded "jiffy bags" and may arrive by post, be delivered by hand or arrive via a courier.

When receiving packages please be aware of any of the following:

Balance - In letter bombs, device components may shift and tend to unbalance an item of mail leaving it feeling "unusual" compared to other items of mail. Such uneven weight distribution occurs because high explosives have a high gram density and are therefore heavier than their volume would suggest.

Sweating – Some chemicals used in explosives may "sweat" and result in "greasy" marks on the envelope or outer wrapping. These should be treated as suspicious.

Odours - Some chemicals may give off unusual odours, for example some devices are constructed of nitrogen based commercial fertiliser. The next time you use garden or lawn fertiliser, note the smell. Nitrogen explosive devices may emit the same odour. Also, a smell of almonds or marzipan should be treated as suspect.

Weight – A letter usually weighs about 28g or under. An effective letter bomb weighs between 50 and 100g; it therefore needs more than the usual value of postage stamps for its size and it is usually thick for a letter, being at least 5mm. On receipt of such a letter, the package should be treated as suspect.

Feel – Letters have a normal "feel". Those that contain devices may simply not "feel" right or may be "stiff". This can indicate the presence of plastic or metallic components.

Packaging – Be very cautious of envelopes or packages, which are found within other packages. This may be an attempt to mask or hide the actual explosive device. Also, be careful if the package is over packed – this could indicate that the bomber has protected the device so that it reaches its target.

Addressing – Be cautious of items marked "To Be Opened Only By", or one which carries a strange place of origin, postmark, script, disguised or unusual writing or type, obvious misspelling or altering of words in the address field, or the lack of a return address. Also, be careful if the address is made up of cut out letters or was written by using stencils

Excessive Postage – The bomb maker will not wish his item to be weighed in a Post Office, so they will probably buy stamps and will affix a higher postage than necessary, not wanting the package to be delayed

Additional sealing – this can be another sign that the bomber has attempted to protect the package and has glued down ends or sticky taped flaps

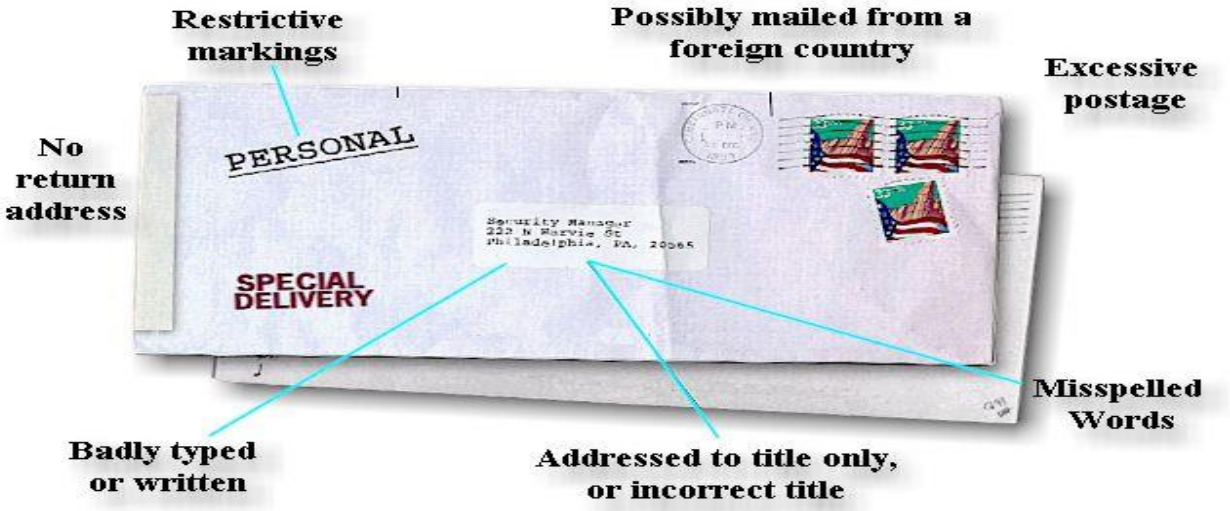
A small hole – if there is a small hole- like a pin hole - in the package wrapping or the envelope the package should be treated as suspect

Tell-tale signs

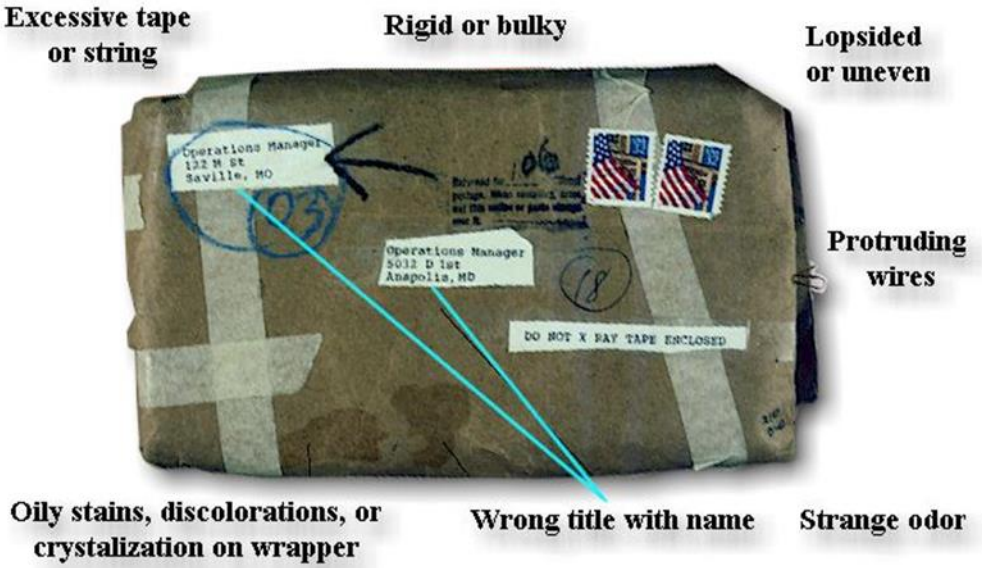
The following are regarded as tell-tale signs off suspect postal/letter bomb:

- Grease marks on the envelope or package
- Unusual odour such as marzipan or machine oil
- Visible wiring or tin foil, especially if the envelope or package is damaged
- Very heavy for its size
- Uneven weight distribution
- Contents rigid in a flexible envelope
- Excessive wrapping
- Poor handwriting, spelling or typing
- Wrongly addressed
- From an unexpected source
- Too many stamps for the weight of the package
- Delivered by hand from an unknown source
- Posted from an unusual place
- Follows a pattern of devices found elsewhere

What makes it a Suspicious Letter?



What makes it a Suspicious Package?



7. Bomb threats

Procedures for handling bomb threats

Most bomb threats are made over the phone and the overwhelming majority are hoaxes, often the work of malicious jokers, although terrorists do make hoax calls with the intent of causing alarm and disruption. Any hoax is a crime and, no matter how ridiculous or unconvincing, must be reported to the police.

Calls may be of two kinds:

- Hoax threats designed to disrupt, test reactions or divert attention
- Threats warning of a genuine device – These may be attempts to avoid casualties or enable the terrorist to blame others if there are casualties. However genuine threats can provide inaccurate information about where and when a device might explode.

Principles

Base bomb threat procedures on the following principles:

Ensure that all staff who could conceivably receive a bomb threat are trained in handling procedures or have ready access to instructions. Switchboard operators should be familiarised with procedures.

Draw up a clear list of actions to follow upon receipt of a call. Even though staff may be unable to assess a threat's accuracy or origin, their impressions of the caller could be important. A Bomb Threat Checklist is circulated with these instructions and should be readily available for staff.

Consider that the member of staff who receives the threat may not be prepared – receiving such a threat may be the closest that many people ever come to acts of terrorism – so offer some basic advice for staff on handling a threat, for example:

1. Stay calm and listen.
2. Obtain as much information as possible – try to get the caller to be precise about the location and timing of the alleged bomb and whom they represent. If possible, keep the caller talking.
3. Ensure that any recording facility is switched on.
4. When the caller rings off, dial 1471 (if that facility operates and you have no automatic number display) to see if you can get their number.
5. Immediately report the incident to the relevant manager or security controller to decide on the best course of action and notify the police. If you cannot get hold of anyone, and even if you think the call is a hoax, inform the police directly. Give your impressions of the caller and an exact account of what was said.
6. If you have not been able to record the call, make notes for the security staff or police. Do not leave your post – unless ordered to evacuate – until the police or security arrive.

8. Evacuation planning

Evacuation should be part of your security plan and Business Continuity Plan (BCP). In some circumstances it may be better to retreat into protected spaces within your building.

You might need to evacuate your premises because of:

- a threat aimed directly at the building
- a threat received elsewhere and passed on to you by the police
- discovery of a suspicious item in the building (perhaps a postal package, an unclaimed holdall or rucksack)
- discovery of a suspicious item or vehicle outside the building
- an incident to which the police have alerted you.

Whatever the circumstances, you should tell the police as soon as possible what action you are taking.

The biggest dilemma facing anyone responsible for an evacuation plan is how to judge where the safest place might be. For example, if an evacuation route takes people right past a suspect device outside your building, or through an area believed to be contaminated, evacuation may not be the best course of action. **You might have to consider the use of protected spaces.**

A general rule of thumb is to find out if the device is external or internal to your premises. If it is within the building you may consider evacuation, but if the device is outside the building it may be safer to stay inside.

The decision to evacuate will normally be yours, but the police will advise. In exceptional cases they may insist on evacuation, although they should always do so in consultation with your Security Controller.

Planning and initiating evacuation should be the responsibility of the Security Controller. Depending on the size of your business and the location of the building, the plan may include:

- full evacuation outside the building
- evacuation of part of the building, if the device is small and thought to be confined to one location (e.g. a letter bomb found in the post room)
- full or partial evacuation to an internal safe area, such as a protected space, if available
- evacuation of all staff apart from designated searchers
- retreat to protected spaces.

Evacuation instructions

Evacuation instructions must be clearly communicated to staff and routes and exits must be well defined. Appoint people to act as marshals and as contacts once the assembly area is reached. Assembly areas should be at least 500 metres away from the incident. In the case of most vehicle bombs, for instance, this distance would put them beyond police cordons - although it would be advisable to have an alternative about 1km away. Car parks should not be used as assembly areas.

Disabled staff should be individually briefed on their evacuation procedures. Many organisations advise the use of firefighter lifts for evacuating disabled staff in the event of an incident.

Suspected letter or parcel bombs

In the case of suspected letter or parcel bombs - evacuate the room and the floor concerned along with the two floors immediately above and below.

CBR incidents

Responses to chemical, biological radiological (CBR) incidents will vary more than those involving conventional or incendiary devices, but the following general points should be noted:

- the exact nature of an incident may not be immediately apparent. For example, an improvised explosive device (IED) might also involve the release of CBR material;
- in the event of a suspected CBR incident within the building, switch off all air conditioning, ventilation and other systems or items that circulate air (e.g. fans and personal computers). Do not allow anyone, whether exposed or not, to leave evacuation areas before the emergency services have given medical advice, assessments or treatment;
- if an incident occurs outside the building, close all doors and windows and switch off any systems that draw air into the building. Agree your evacuation plan in advance with the police and emergency services, the local authority and neighbours. Ensure that staff with particular responsibilities are trained and that all staff are drilled. Depending on the type of incident, you may need to agree with the police what action you take. Building managers should ensure that they have a working knowledge of the heating, ventilation and air conditioning systems and how these may contribute to the spread of CBR materials within the building.

Protected Spaces

Evacuation is never advisable if there is a general threat and the building has a protected space.