

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY



Policy Statement

SCCS Survey Equipment Limited aims to raise awareness of potential security threats and terrorist related activities and minimise these wherever possible to provide a safe working environment for all employees. The purpose of this policy and associated procedures is not to be alarmist or cause undue fear or anxiety, but rather to be proactive, prepared and ensure staff understand their roles and responsibilities should a situation arise

Policy Aim & Commitments

Company Commitments:

- Compliance with all UK legislative requirements including Counter Terrorism Legislation put in place by any Government body.
- Review of risk management controls.
- Effective roll out & communication of any safety measures implemented.

Employee Commitments:

SCCS personnel shall be required to observe and comply with the following obligations:

Take reasonable care for the health & safety of themselves and other persons who may be affected by their acts or omissions whilst at work in accordance with all Company Health & Safety Policy, training and other guidance.

Policy Aims:

- To raise awareness throughout the company of potential security threats
- To raise awareness throughout the company of possible targeting by terrorist groups
- Provide a clear set of expectations and instructions to all employees of the procedure to follow should a security threat arise

Scope

This policy applies to:

- All SCCS personnel.
- Visitors to and contractors working on SCCS premises.
- SCCS personnel engaged in work activities off SCCS premises.

Definitions

- "Company" shall mean SCCS

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K.Smith

- “VAW” shall mean Vehicle as Weapon attack.
- “CBR” shall mean Chemical, biological or radiological materials.

1. Legal Requirements Applicable

The Control of Explosives Precursors Regulations 2014

The Export Control Order 2008

2. Recognising Potential Threats

The UK nationally faces a range of threats to its security. There is a serious and sustained threat from international terrorism to the UK and UK interests overseas. The current threat level in the UK can be found on the MI5 website (www.mi5.gov.uk). Threat levels will be classified as one of the following:

- LOW – means an attack is highly unlikely.
 - MODERATE – means an attack is possible, but not likely.
 - SUBSTANTIAL – means an attack is likely.
 - SEVERE – means an attack is high likely.
 - CRITICAL – means an attack is highly likely in the near future.
- SCCS, its staff and assets could face a range of threats, both direct and indirect which can range in seriousness from low key to critical.
 - Direct threats are those where SCCS itself is the target
 - Indirect threats are those where the company was not the target but must deal with the consequences.

Direct Threats

- SCCS deals in items, such as Lithium Ion batteries, that could be deemed harmful in large quantities. Information on these products is widely available and listed on our website.
- SCCS supplies GPS equipment and drones. This kind of positioning/measuring equipment could have a dual purpose and be used for terrorist activity.
- We also have potentially hazardous chemicals such as Isopropanol and methylated spirits on site, that we are able to purchase from suppliers and could be asked to supply for a customer.
- A member of a terrorist organisation could attempt to infiltrate the company by being recruited.

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K.Smith

- Alternatively, a terrorist group may target an existing employee in an attempt to indoctrinate them and recruit them into carrying out business for the group.
- The SCCS Head Office and staff could be at risk from a physical attack by either a terrorist group or Lone Wolf attack which could involve bombs/letter bombs being placed in the building.
- SCCS run a fleet of small and medium size commercial vehicles. These have been commonly used in recent 'vehicles as weapons' attacks around the world.

Indirect Threats

- The SCCS commercial delivery vehicles operate in city centres on a daily basis. On average 3 of them are in central London including increased risk areas such as Westminster and Canary Wharf.
- IT Networks are always at risk from hackers or potential new viruses.

3. Identifying Vulnerabilities

People

- Staff – any direct threat to the company is a direct threat to its staff. Delivery drivers are at risk when out on the road, particularly if they are operating in potentially targeted, highly populated areas such as Central London
- Visitors, customers and contractors – anyone visiting Head Office would also be at risk if there were a physical attack on the building.
- Members of the public – Any member of the public around Head Office could be at risk during an attack. If a fleet vehicle was used as a weapon this would also be a risk to anyone in the vicinity of the vehicle at the time.

Physical Assets

- Buildings - SCCS only has one building, its Head Office at Alpha Drive, Eaton Socon. This building houses its office and administration operations as well as a workshop and warehouse facility.
- Vehicles – SCCS has a fleet of small and medium sized commercial vehicles that deliver and collect equipment nationwide. These could be targeted by thieves either for the vehicles themselves, or their contents. They could also be exploited to aid terrorists in a 'vehicles used as weapons' attack.
- Equipment – SCCS deals in surveying equipment. Some kit is of extremely high value and if people are familiar with it, they will know its worth, it can therefore be targeted by thieves in the area of delivery knowing that construction sites take deliveries of such equipment. It can also be targeted where it is stored in our warehouse/head office facility.

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K.Smith

Information and Processes

- IT Systems – All IT networks are managed centrally by our parent company Hexagon AB. It could be at risk of hacking from someone targeting SCCS, or the Hexagon Group as a whole.

4. Security Measures and Procedures

Supply of harmful goods

- As a company SCCS supply goods that are potentially harmful in large quantities and can be used in activities such as bomb making. To avoid supplying potentially harmful goods to possible terrorists/activist groups due diligence must be carried out on all new customers including credit checks and trade references.
- Any suspicious transactions relating to regulated substances are to be reported to the national contact point as required by The Control of Explosives Precursors Regulations 2014.
- Any unusually large quantities of potentially harmful goods i.e. restricted chemicals or lithium ion batteries are to be red flagged and treated as above.
- Before shipping any goods, the member of staff who is processing the sale will check the Government website for any existing trade restrictions in place with that country. This list can be found at <https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions> as a back up to this our shipping company, MartinTrux, have very good knowledge of trade sanctions and can be relied upon to advise if the shipping of goods to that destination is allowed.
- Our sales team will also check the destination is not listed by Hexagon as a country that we do not trade with.
- SCCS always comply with export control rules and obtain the correct export licence if needed in the export of controlled goods.

Employment of those involved in Terrorist Activity

- SCCS follows the Hexagon Recruitment Policy, carried out by Human Resources.
- As part of the recruitment policy there is a screening process. The following must be completed before any employee commences employment:
 - Complete a new starter form.
 - Provide Right to Work in the UK documentation such as a passport.
 - 5 years employment referencing
 - 2 proofs of home address (dated within the last 3 months)
- All prospective employees are subject to provide 2 satisfactory employment history references, including all countries that the applicant has resided in for over 6 months, in the last 5 years.

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K.Smith

- All prospective employees who will be driving as part of their role must provide a copy of their current valid driving licence as detailed in 014.9.2014.PL Company Driving and Vehicle Policy.
- Should there be any gaps in a person's employment history, or any part of their employment history you are unable to verify they must supply a suitable character reference from a person who has known them for 5 years and is an accredited professional.
- All prospective employees are required to produce verification of their identity either by producing a UK passport or alternatively a full birth certificate AND Photo ID. SCCS are required to copy and retain the photographic evidence on the employee's personal file.
- A confidential reporting system is in place to ensure that if members of staff have suspicions that a colleague is involved in or being indoctrinated into a terrorist organization, they are encouraged to report it.
- Always speak to your Line Manager as your first point of contact. If you feel unable to speak to them you can speak to any member of the Senior Management or Vicky Stallan (HR)
- There may be some cases where no wrongdoing is found through internal procedures. Protection will be given, and no disciplinary action taken if the disclosure is reasonable, made in good faith and the information believed to be true.

Physical Attack at Head Office

Letter Bombs

- Terrorists and others wishing to cause harm or disruption have long used postal and courier services to deliver hazardous items to target recipients. Delivered items can include letters, packets and parcels and may contain:
 - explosive or incendiary devices
 - sharps or blades
 - offensive materials
 - chemical, biological or radiological (CBR) materials or devices.
- Although any suspect item should be treated seriously, remember that the great majority will be false alarms, and a few may be hoaxes.
- A delivered item will probably have received rough handling in the post and so any device is unlikely to function through being moved, but any attempt at opening it may set it off. In contrast, even gentle handling or movement of an item containing CBR material can lead to the release of contamination. Unless delivered by courier, an item is unlikely to contain a timing device.
- Delivered items come in a variety of shapes and sizes; a well-made one will look innocuous but there are many possible indicators that a delivered item may be of concern:
 - a padded envelope ('Jiffy Bag') or other bulky packaging

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K. Smith

- additional inner envelope or other contents that may be difficult to remove.
- labelling or excessive sealing that encourages opening at a particular end or in a particular way.
- oddly shaped or lopsided
- envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges)
- marked 'to be opened only by' 'personal' or 'confidential'.
- unusual origin postmark and/or return address or no postmark/return address.
- no return address or return address that cannot be verified
- poorly or inaccurately addressed or address printed unevenly or unusually.
- more stamps than needed for size/weight of package.
- greasy or oily stains emanating from within.

Additional explosive or incendiary indicators:

- unusually heavy or uneven weight distribution
- small hole(s) in envelope or wrapping.

Additional CBR indicators:

- powders, liquids or odours emanating from package.
 - wrapping stained by liquid leakage
 - unexpected items or materials found in package on opening (loose or in a container): powdered, crystalline or granular solids; liquids; sticky substances or residues.
 - unexpected odours observed on opening.
 - sudden onset of illness or irritation of skin, eyes or nose
- Bulky deliveries (e.g. office equipment) can be a potential vulnerability. SCCS aims to reduce risk by only using trusted suppliers wherever possible and inspecting deliveries.
 - Staff who open significant volumes of post should do so with letter openers and with minimum movement, hands are to be kept away from noses and mouths and always wash their hands after such work.
 - Staff should not blow into envelopes or shake them.

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K. Smith

- If a suspect letter/package is received, the member of staff who has discovered it, or somebody else in the vicinity, should sound the fire alarm to evacuate the building in line with the emergency evacuation policy.

Bomb Threats

- Most bomb threats are made over the phone. The overwhelming majority are hoaxes, often the work of malicious pranksters, although Irish Republican terrorists have also made hoax calls in the past.
- All staff could conceivably receive a bomb threat and need to have a good awareness of these handling procedures:
 - stay calm and listen.
 - obtain as much information as possible - try to get the caller to be precise about the location and timing of the alleged bomb and try to establish whom they represent. If possible, keep the caller talking.
 - Make a note of any number showing on the automatic number display on your phone – if no number shows when the caller rings off, dial 1471 to see if you can retrieve their telephone number.
 - We do not currently have a facility to record calls so, if possible, make notes about what the caller sounds like (sex, age, any accent) any background noise (outdoor, vehicles, other people talking) and the exact wording they use in the bomb threat.
- Immediately tell Lucy Walker (FORS Counter Terrorism Champion) or Roz Wankling (Health & Safety Manager) or someone from Senior Management. It is their responsibility to decide on the best course of action and who should 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 them your impressions of the caller as well as an exact account of what was said.

Group or Lone Wolf Attacks

- Access to Alpha House is controlled by a magnetic lock on the second set of doors into the building. This can only be unlocked from the outside by authorized personnel using their allocated fob.
- The programming of EntrySign access fobs is controlled by Roz Wankling (Health & Safety Manager)
- If you have a visitor coming to Alpha House they can be pre-programmed into the EntrySign system. They can enter through the first set of doors into the porch area of the building, use the EntrySign podium to sign themselves in and this will then send an email to the SCCS employee they are visiting to alert you your visitor is here. You can then go down and let them into the building. To pre-book a visitor see Roz Wankling (Health & Safety Manager)

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K.Smith

- If you see someone in the porch area of Alpha House do not give them access to the building until you have questioned who they are visiting and confirmed this with the member of staff.
- In the rare event of a firearms or weapons attack at Head Office staff are to follow the advice from the National Counter Terrorism Policing (NCTPHQ) Action Counters Terrorism (ACT) campaign and:

RUN, HIDE, TELL

- **RUN** – to a place of safety. This is a far better option than to surrender or negotiate. If there's nowhere to go, then
 - **HIDE** – its better to hide than to confront. Remember to turn your phone to silent and turn off any vibrate mode. Barricade yourself in if you can. Then finally and only when it is safe to do so
 - **TELL** – the police by calling 999
- If hiding whilst making a 999 call it may be dangerous to speak, in which case you should use the system called Silent Solutions which helps callers who cannot speak to an operator.
 - A silent 999 call will not produce an emergency service response. To summon help you should do the following:
 - Dial 999
 - Listen to the operator's questions
 - If possible, cough or make another noise to let the operator know you are there
 - Then dial "55" on your keypad to summon help
 - If no noise is made and 55 isn't keyed in, the call handler will assume it's an accidental call and hang up

Vehicles as Weapons Attack (VAW) and Vehicle Security

- The use of vehicles as a weapon, and vehicle-borne improvised explosive devices, to injure and kill people has become a real threat in recent years, which means SCCS as operators of commercial vehicles need to act to secure our vehicles and protect our staff.
- SCCS strives to promote a strong security culture which will help mitigate security risks, including VAW by promoting compliance with security measures, awareness and vigilance.
- All drivers of commercial vehicles are to complete the FORS Online training module in Security and Counter Terrorism to help raise awareness and recognize potential threats.
- SCCS personnel will be responsible for ensuring any vehicle used for Company business is suitably secure & locked when unattended. This includes during loading and unloading and when taking breaks.

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K. Smith

- If possible, lock the doors of your vehicle when you are moving. This helps protect you from physical attack at times you could be vulnerable such as in slow moving traffic or stationary at lights/junctions.
- A second key for every company vehicle is to remain with the Group Fleet Manager who will ensure they are under restricted access.
- Any vehicles left on SCCS property overnight must be in a designated parking bay so that they can be securely locked on site by the security guard, using the car park barrier.
- When loading or unloading your vehicle either on SCCS property or customer site, remain vigilant for unauthorized personnel.
- Never take unauthorized passengers in your vehicle as this is a serious breach of security and leaves loads and vehicles open to theft and drivers open to risk of attack.
- When out on deliveries drivers must follow advice of the local police force during events, demonstrations, parades etc.
- In the event of the theft of your vehicle or load contact the police on 999.
- If you have any concerns over suspicious activity or potential crime you can contact 101 – non-emergency crime or the Anti-Terrorism hotline on 0800 789 321.
- If you are with/in your vehicle and are the victim of a theft, or you witness a theft from your vehicle you **MUST NOT** try to approach or stop the thief or get into any altercation.
- If you are threatened whilst in or around your vehicle comply with the instructions of the person threatening you in order to keep yourself safe.
- If you suspect a vehicle-borne improvised explosive device has been fitted to your vehicle, you must evacuate your vehicle and contact the authorities.
- **NEVER PUT YOURSELF IN DANGER.** SCCS values its staff, and the company wants all of its employees to be safe at work.

IT Security

- All IT networks are managed centrally by our parent company Hexagon AB and as such security measures are put in place by them.
- All Incidents are handled via the ticketing tool “ServiceNow” according the assigned priority (impact/urgency). There are special processes for Major Incidents (Priority 1)
- Various Security Tools are in place to guard against cyber-attacks. Sentinel One as advanced endpoint protection, F5 as Application Firewall, Skyhigh as CASB, Nextthink as additional end point monitoring / analytics.
- Sporadic penetration-tests are conducted by external consultants.

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K.Smith

- Security patching policy and procedures uses Windows Update Service (WSUS) for Windows Updates and for 3rd party Ivanti DSM Patch Management.
- All staff must complete mandatory IT Security training issued by Hexagon AB. This covers subjects such as cyber security and risks training, ransom ware attacks, laptop security and hacking.

5. Reporting

Any event/incident involving a security or terror threat must be reported through the appropriate channels .

Reporting of Non-Physical Attack

- Any security threat that doesn't involve an attack from a physical person, such as a Letter Bomb or phone call should be reported immediately to either Lucy Walker (FORS Counter Terrorism Champion) or Roz Wankling (Health & Safety Manager).
- Try to make notes/report on the following:
 - Who and/or what was witnessed?
 - When it was seen?
 - Where it was seen?
 - Why it was suspicious?
- Lucy and/or Roz will then discuss the threat and any action that should be taken with members of the Senior Management team and decide if the incident needs to be reported to the authorities, and if so, who best to report it to:
 - 999 – for an emergency response from the police
 - 101 – for anything not requiring an emergency response
 - 0800 789 321 – police anti-terrorist hotline for any situation with an immediate threat to life or property
- Lucy and/or Roz will then report the incident to the relevant authorities if it is deemed necessary.
- They will then communicate action/advice from the authorities back to the Senior Management team to then filter out to all employees if necessary. Consideration will be given to not revealing sensitive information that has the potential to assist other attackers or cause unnecessary alarm to employees or the general public.

Reporting of Physical Attack

OPERATIONAL SECURITY & COUNTER TERRORISM POLICY

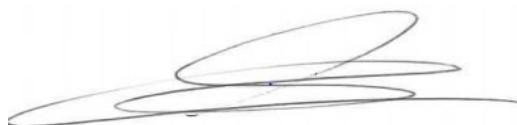
Policy Reference:	014.13.2020.PL
Revision No:	4
Date of 1 st Issue:	09/12/2020
Date of Revision:	04/12/2023
Reviewed by:	L. Walker
Approved by:	K.Smith

- If you are the victim of a physical attack at Head Office you must follow the Run, Hide, Tell approach as detailed above.
- If possible, raise the alarm by using the fire alarm to evacuate the building.
- If raising the alarm will put yourself at risk, then you must not do it. Instead run and hide.
- If possible, contact the emergency services on 999, using 55 to make a silent alert for help if needed.
- If you are the victim of a physical attack whilst out in a company vehicle, if they have gained access to your vehicle you MUST evacuate.
- If possible, raise the alarm to anybody in the vicinity.
- If alerting others to the situation puts yourself at risk, then you must not do it. Instead run and hide following the procedure detailed above.

6. Compliance & Review

- Overall responsibility for ensuring compliance with this policy will rest with the Senior Management Team.
- Day to day responsibility for facilitating and administering compliance with this policy will be delegated as appropriate.
- SCCS personnel shall be responsible for compliance with this policy. Any personnel failing to comply with the remit of this policy may be subject to disciplinary action.
- This policy will be reviewed at minimum annually, after a change of operational procedure, and as response to a potential security or terrorism threat.
- Any review must consider future security measures and improvements, staff communication and training requirements to ensure a continuous improvement process.

Signed:



Print name:

Kevin Smith

Position:

Managing Director

Date:

04/12/2023

Revision

4

Next review:

03/12/2024