NHS
Bradford District and Craven
Clinical Commissioning Group

Security management policy

Key information

Responsible director:	Strategic director of organisation effectiveness
Author:	Roberto Giedrojt, BDCFT health and safety
Approval body:	Audit and governance committee
Date approved:	2 November 2020
Version:	V1.0
Review date:	November 2023

Version control

VNo.	Date	Author	Description	Circulation
V1.0	October 2020	R. Giedrojt, BDCFT	Version approved by audit and governance committee	CCG wide

Contents

1 Introduction

Bradford District & Craven Clinical Commissioning Group (BD&C CCG) is committed to ensuring effective arrangements for the personal safety of staff, patients and visitors to their property and the property and premises of the organisation.

BD&C CCG has responsibilities under the health and safety at work act 1974, particularly in relation to employees ensuring, as far as is reasonably practicable, the health, safety and welfare of employees at work.

The management of health and safety at work regulations 1999 require employers to assess risks to employees and nonemployees and make arrangements for effective planning, organisation, control, monitoring and review of health and safety risks.

Responsibility for security rests with all persons working within BD&C CCG**.**

2 Scope of the policy

The policy applies to BD&C CCG and all their employees and must be followed by all those who work for the organisations, including the governing body, senior leadership team, those working for commissioning support services, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

Independent contractors are responsible for the development and management of their own procedural documents and for ensuring compliance with relevant legislations and best practice guidance.

3 Associated documentation

This policy should be read in conjunction with the following associated documentation:

- integrated risk management framework
- incident reporting policy
- incident management, investigation and reporting procedure
- health and safety policy
- lone worker policy (including violence and aggression)
- anti-fraud, corruption and bribery policy
- standing financial instructions
- business continuity plan

4 Policy statement

BD&C CCG will provide and promote as far as is reasonably possible, a safe and secure environment for all staff, service users, visitors and contractors.

5 Aims and objectives

BD&C CCG will:

- provide and promote as far as reasonably possible, a safe and secure environment for all staff, service users, visitors and contractors
- establish acceptable levels of risk on its premises and for its employees
- develop systems and processes to help to ensure the safety of staff at work
- develop procedures to deal with reports of crime, threats and damage

- raise security awareness within the organisation
- identify security trends and react quickly to remove or reduce risk

6 Duties, accountabilities, roles and responsibilities

6.1. Duties within the organisation

6.1.1 Governing body

The governing body is responsible for ensuring that the necessary support and resources are available for the effective implementation of the security management policy.

The governing body will also be responsible for the establishment of effective control over its resources through adequate procedures and management practices and for ensuring that all activities meet current legal requirements.

6.1.2 Chief officer

The chief officer is the accountable officer and has ultimate responsibility for security within the organisation.

The chief officer is responsible for ensuring that there is expert up to date security advice and services available within the organisation. They will also be responsible for ensuring that effective systems and practices are in place to maximise security throughout the organisation and for promoting preventative security measures in accordance with the previous recommendations of NHS protect.

6.1.3 Strategic director of organisation effectiveness

Responsibility for security is delegated to the strategic director of organisation effectiveness. As such the strategic director of organisation effectiveness functions as the security management director and has lead responsibility for the development and strategic review of security within BD&C CCG.

6.1.4 Associate director of organisation effectiveness

On behalf of the strategic director of organisation effectiveness, the associate director of organisation effectiveness is responsible for:

- the formulation, implementation and maintenance of an effective security management policy, (following previous NHS protect guidance) in consultation with staff representatives, and ensuring that managers coordinate and implement the policy in their respective areas
- leading security management within BD&C CCG and identifying initiatives for improving security across the organisation
- monitoring the performance of BD&C CCG with regard to the implementation of this policy

6.1.5 On call director

The on call director is responsible for leading on any out of hours security management issues, or if the lockdown procedure or suspicious package / bomb threat procedure is enacted (see appendices two and three).

The decision to evacuate a BD&C CCG building should be made by the on call director after consultation, where possible, with others, e.g. police and members of the senior leadership team.

6.1.6 Heads of service and managers

Individual heads of and managers are responsible for promoting security within their areas of responsibility. In particular they will be responsible for:

- ensuring that they and their staff are trained so that they are familiar with the content of the security management policy and associated procedures
- undertaking risk assessments of their areas of responsibility and acting to remove / reduce as far as possible any security risks identified
- keeping inventories of departmental property
- ensure that staff who travel as part of their role are aware of, and comply with, the requirements that the motor vehicle they use is covered by a relevant insurance policy which provides cover while the vehicle is on official business including cover against risk or injury, and that where appropriate, the vehicle has a valid MOT certificate. The driver should also have an appropriate driving licence and is not aware of any reason why they should not safely and legally drive a vehicle
- see also the lone working policy for responsibilities related to the management of lone workers

6.1.7 Provider of security management services

The overall objective of the provider of security management services Bradford District Care Foundation Trust (BDFCT) health, safety and security team is to support BD&C CCG through an advisory function to deliver an environment that is safe and secure.

The BDCFT health, safety and security team will advise BD&C CCG of any requirements, statutory or other, by the preparation of procedures for dealing with crime prevention, supply of security systems and maintenance.

Any security incidents should be reported through the CCG incident reporting procedure.

The BDCFT health, safety and security team will advise and support BD&C CCG in any dealings with the police in pursuing actions against individuals who commit a violent act against a member of staff or in relation to theft or damage of BD&C CCG property.

The BDCFT health, safety and security team will complete an agreed work plan, including an annual security review of all BD&C CCG sites.

6.1.8 All employees and those working on behalf of the CCG

All employees and those working on behalf of the organisation have responsibility for:

- taking reasonable steps to ensure their own personal security and that of colleagues, patients, visitors and the general public
- ensuring that effective measures are taken to ensure that the organisation's premises and property are maintained in a secure condition
- taking steps to safeguard against loss of the organisation's property
- having awareness of and complying with all the organisation's policies and procedures
- taking all reasonable steps to ensure security of their own personal possessions the organisation takes no responsibility for personal possessions
- staff who travel as part of their role are aware of, and comply with, the requirements that the motor vehicle they use is covered by a relevant insurance policy with provides cover while the vehicle is on official business including cover against risk or injury, and that where appropriate, the vehicle has a valid MOT certificate. The driver should also have an appropriate driving licence and not be aware of any reason why they should not safely and legally drive a vehicle

6.1.8 Visitors and contractors

All visitors and contractors have a general responsibility to give due consideration to security issues and must follow the security procedures of the organisation. All visitors and contractors have a general responsibility to take all reasonable steps to ensure security of their own personal possessions.

BD&C CCG will not accept responsibility or liability for personal property brought into its premises.

6.2. Responsibilities for approval

This policy document will be approved by the audit and governance committee.

7 Policy details

7.1 Incident reporting

Any security incidents should be reported through the CCG incident reporting procedure. IR1 (incident reporting forms) can be found on the intranet and should be sent to the corporate governance team when completed. The governance team will forward all security related incidents to the BDCFT health, safety and security team. IR1 forms should be completed as soon as is practically possible after the incident is identified.

The CCG incident reporting policy and incident management, investigation and reporting procedure can be found on the intranet.

8.2 Personal security

BD&C CCG will, as far as is reasonably possible, work to ensure the personal security of all individuals whilst undertaking work on behalf of the organisations or receiving services from the organisations. It is the responsibility of individuals to take all reasonable steps to ensure that they do not compromise their own security or that of others.

8.3 Lone workers

All reasonable steps will be taken to ensure the safety of employees who, in the carrying out of their job responsibilities, may be required to work alone. This will be achieved by the development of appropriate procedures and working practices and ensuring that staff have the appropriate skills and equipment to enable them to work safely and securely. BD&C CCG lone working policy (including violence and aggression) can be found on the intranet.

8.4 Violence and aggression

BD&C CCG believes that all staff and members of the public have a duty to treat each other with dignity and respect and to behave in an acceptable and appropriate manner. Staff have a right to work, and patients have a right to be treated, free from fear of assault and abuse in an environment that is properly safe and secure.

The health and safety at work act 1974, management of health and safety at work regulations 1999 requires that employers have a duty to ensure the health, safety and welfare of their staff.

Within the NHS there are two definitions identifying physical and nonphysical assault and one further health and safety executive definition related to violence. They are:

- physical assault ‘the intentional application of force to the person of another, without lawful justification, resulting in physical injury or personal discomfort’

- nonphysical assault 'the use of inappropriate words or behaviour causing distress and / or constituting harassment'
- 'any incident, in which a person is abused, threatened or assaulted in circumstances relating to work. This can include verbal abuse or threats as well as physical attacks'

Further guidance is available in the BD&C CCG lone working policy including violence and aggression which can be found on the intranet.

8.5 Crime Prevention

Proactive crime prevention and security awareness will help to ensure a safe, secure environment**.** Staff should make every effort to counter the threat of crime, as follows:

- all suspicious activity must be reported. Any occurring on BD&C CCG premises should be reported to a line manager and an incident reporting form (IR1) completed and returned to the corporate governance team (who will forward to the BDCFT health, safety and security team)
- all incidents of crime must be reported, to the police and, via an IR1 form, to the corporate governance team (who will forward to the BDCFT health, safety and security team)
- all significant items of property belonging to the CCGs must be clearly marked / labelled
- missing items must be reported to line managers
- personal valuables must be kept secure, out of sight and not left unattended
- offices and other rooms must always be left secure. All windows must be closed at the end of the working day

8.6 Assets

The organisation is committed to ensuring the security of all the assets of BD&C CCG including land, buildings, plant and equipment. It is essential that sufficient equipment is available for use at all times and therefore all personnel have a responsibility for ensuring that the organisation's items that they use during the course of their work (e.g. mobile phones, laptops, ipads) are kept safe and secure and are protected from the possibility of theft. BD&C CCG issued equipment should not be left unattended in parked vehicles.

8.7 Security of cash

Cash from all sources throughout the organisation should be held in a secure place and must be deposited with the finance team (at scorex house) or the admin team (at millennium business park).

Petty cash must also be held in a secure place and records must be kept to demonstrate that any use of petty cash conforms to the organisations financial guidance and procedures.

Cash must be stored in a safe. A safe is available in the finance department (at scorex house) and at millennium business park (managed by the admin team). Access to the safe is managed by and limited to authorised staff only.

The use of petty cash and BD&C CCG safes are governed by standing financial instructions.

8.8 Personal property

Whilst BD&C CCG do not take responsibility for the security of the personal property of staff, patients, visitors or contractors, reasonable steps will be taken to ensure that

systems and processes are in place to help individuals to take responsibility for their own possessions.

Staff are advised that valuables and other personal property with high sentimental value must not be brought to work.

8.9 Identification badges

All staff must wear their issued identification (ID) badges whilst on BD&C CCG business. Lost or stolen ID badges must be reported to human resources as soon as possible and must be logged as an incident using an IR1 form. Faded ID badges must be replaced.

Visitors and contractors must report to the appropriate reception area and (at scorex house only) collect a visitors / contractors badge to be identifiable on the premises. For health and safety purposes, this is supported by a signing-in and signing-out register at both scorex house and millennium business park.

Staff are advised to challenge any unknown individual, who is present within the work place without the appropriate identification, to report suspicious behaviour and prevent unauthorised entry to the building by “tailgating” (unauthorised entry gained to premises without the use of an appropriate ID pass and facilitated by pass holders).

ID badges must be recovered on the termination or suspension of employment or contract and any records updated accordingly.

8.10 Control of locks, keys and access control systems

Access control systems can be put in place to help protect people, property and assets in the NHS. Proper access controls that staff use and have confidence in can help deter and prevent security related incidents. Essentially, they should be designed to ensure that members of staff, patients and the public only have access to areas they need to enter.

All keys must be kept secure and along with access code details, should only be made available to bona fide personnel. Procedures and systems must be in place to ensure that appropriate records are kept of the whereabouts of keys that are available for use by a number of different staff (note: a key holders list is available in the on-call pack)

Lost or missing access control fobs (applicable at scorex house only) must be reported as soon as possible to NHS property services who will then delete the record from the access control system’s database to prevent security breaches.

Any system is only as good as the people who use it. Staff must adhere to procedures on access and the use of such equipment. For example, staff must not lend access cards to others or wedge doors open and to be aware of the possibility of tailgating. Where number pads or similar locking devices are used, managers and staff should also be required to change codes on a regular basis and not divulge the codes to those who are not entitled to access those areas.

Access control systems are electronic systems and record movement of staff to a database. The database is the property of BD&C CCG and could be reviewed in support of internal and external investigations. Appropriate authorisation to review such data is required from the senior information risk officer (SIRO) or caldicott guardian.

Through the use of risk assessment and crime prevention surveys, the local security management specialist and NHS property services can identify those areas of greatest risk where access controls should be in place.

8.11 Smart cards

Smart cards allowing SystemOne and / or ESR access be should kept secure at all times. Smart cards should not be left in a computer when not in use.

Lost or stolen smart cards must be reported to registration.authority@this.nhs.uk as soon as possible and must be logged as an incident using an IR1 form.

8.12 Closed circuit television (CCTV)

Closed circuit television (CCTV) is a means to aid the deterrence and detection of crimes and other incidents.

There is currently no CCTV within BD&C CCG premises. In the area around scorex house there is significant CCTV presence.

Should the CCGs choose to install CCTV within the BD&C CCG premises, a robust procedure defining its operational requirements will be developed to ensure any such system is efficient, effective and legal. This is because CCTV is an intrusive measure which infringes individual privacy.

Any future CCTV system will be properly maintained and will be managed in accordance with the BD&C CCG confidentiality and data protection policy and access to records (subject access request) procedure. As such signs will be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.

8.13 Data security

The SIRO will be responsible for the development and implementation of security systems to ensure the security of the organisation's electronic data / information systems and to ensure compliance with current legislation and guidance. Please refer to the BD&C CCG suite of information governance / data security and protection policies and procedures available on the BD&C CCG intranet and website.

8.14 Car parking security

Vehicles and their contents which are left on property occupied by BD&C CCG are left at the owners own risk. BD&C CCG issued equipment or confidential information should not be left unattended in parked vehicles.

Users of bicycles are strongly advised to ensure the security of their bicycles by the use of chains and / or clamps. All removable items such as wheel pumps should be removed from the bicycles and paniers should be locked. All bicycles brought onto BD&C CCG premises should be insured and security engraved. The BD&C CCG accept no liability for bicycles parked or left on its premises.

8.15 Building lockdown

Lockdown is the process of preventing freedom of entry, exit and movement around a BD&C CCG or other specific building / area, in response to an identified risk, threat or hazard that might impact upon the security of staff or indeed the capacity of that facility to continue to operate. Lockdown procedures may be activated in response to any number of situations, but some of the more typical might be:

- a reported incident / civil disturbance in the local community (with the potential to pose a risk to staff in the building)
- an intruder on the premises (with the potential to cause a risk to staff)
- a warning being received regarding a risk locally, of air pollution (smoke plume, gas cloud etc)
- the close proximity of a dangerous animal roaming loose

See appendix two for the lock down procedure.

8.16 Suspect packages and bomb threats

Packages and letters delivered by the royal mail and other courier services to BD&C CCG premises also pose a potential threat. Guidance is supplied to staff giving details on the procedure for opening post (see appendix three). This procedure is also aimed at assisting all staff who handle post in assessing the risks faced from postal threats and implementing appropriate screening and security measures. Guidance for this procedure has been sought via (PAS) 97: 2015 mail screening and security specification, produced by the centre for the protection of national infrastructure in collaboration with the British standards institute.

Appendix three also sets out the procedure to be followed in case of a bomb threat being made.

8.17 Major incidents and contingency planning

The civil contingencies act 2004 is important legislation providing a statutory and regulatory framework for resilience in the UK. The act delivers a single framework for civil protection in the UK and sets out clear expectations and responsibilities for front-line responders at the local level, to ensure that they are prepared to deal effectively with the full range of emergencies from localised incidents to full-scale emergencies.

As outlined in the act, BD&C CCG are category two responders and are part of those organisations that support the key emergency category one responders in any emergency response (e.g. fire, police, ambulance, local authorities and NHS acute trusts). They are subject to a set of civil protection duties and are required to put in place business continuity plans and cooperate with category one responders. These plans include robust security arrangements that detail the role and responsibilities of security officers during the course of localised incidents and full scale emergencies.

8.18 Increase in security measures in response to national threat levels

As threat levels increase, security measures will need to be reviewed to ensure they provide the appropriate protection and assurance. Appendix four highlights the key actions to be taken in response to any notification on an increase in the threat level.

9 Dissemination, implementation and training

This policy will, following ratification by the audit and governance committee, be disseminated to staff, governing body and senior leadership team members via the staff briefing process.

The policy can be accessed via the CCG intranet and website.

Any staff or managers who feel they require any specific training on the contents of the security management policy should contact the BDCFT health, safety and security team in the first instance to discuss their training needs.

10 Review and monitoring

The policy will be reviewed every three years or when procedural, legislative or best practice changes occur.

Compliance with the security management policy will be monitored by the audit and governance committee via incident reporting and updates from the BDCFT health, safety and security team.

11 Public sector equality duty

The Equality Act 2010, available on the GOV.UK website, includes a general legal duty to:

- eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the act
- advance equality of opportunity between people who share a protected characteristic and people who do not share it
- foster good relations between people who share a protected characteristic and people who do not share it

The protected characteristics are:

- age
- disability
- gender reassignment
- marriage or civil partnership (only in respect of eliminating discrimination)
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

Public bodies have to demonstrate due regard to the general duty. This means active consideration of equality must influence the decisions reached that will impact on patients, carers, communities and staff.

It is no longer a specific legal requirement to carry out an equality impact assessment on all policies, procedures, practices and plans but, as described above, BD&C CCG do need to be able to demonstrate they have paid due regard to the general duty.

The policy sets out BD&C CCG overall approach to security management and aim to provide a safe and secure environment to protect staff, visitors, contractors and assets of BD&C CCG. It is not believed that this policy will impact on or affect differently or adversely any of the groups with protected characteristics.

13 References

- NHS protect standards (these are now legacy standards following the disestablishment of NHS protect)
- (PAS) 97: 2015 mail screening and security specification, centre for the protection of national infrastructure

14 Appendices

1. security contacts
2. building lockdown procedure
3. suspect packages and bomb threat procedure
4. increased national threat level procedure

Appendix 1: Security contacts

In all emergency situations the police must be contacted first on: 999

Managers are responsible for circulating appropriate security contact details to their staff and ensuring staff are aware of the local security arrangements.

Staff working in the community must agree local lone working emergency contact procedures within their own departments in accordance with BD&C CCG lone working policy.

Working hours security contact details:

HealthandSafetyHelpDesk@bdct.nhs.uk, 01274 228356

Staff Name	Job Title	Contact Number
Dan Casey	Health, safety and security co-ordinator	07703 378 146
Roberto Giedrojt	Health, safety and security officer	07718 421 980
Gillian Grice	Health, safety and security co-ordinator	07841 763 642
Claire Bardgett	Health, safety and security co-ordinator	07715 040 736

Out of hours support:

Emergency calls for immediate support must be directed to the police on 999.

Non emergencies can be reported to the police on 101.

Any out of hours security incidents should be reported to BD&C CCG director on call via the lynfield mount hospital switchboard, 01274 494194.

Appendix 2: Building lockdown procedure

The purpose of this procedure is precautionary but puts the building in a state of readiness (whilst retaining a degree of normality) should a situation escalate.

The following actions will be implemented during a lockdown:

Lockdown arrangements

- set the outer building door to the off position from the control panel located on the reception desk (scorex house) - or, lock the external door manually (millennium business park) – or the required actions to manage access control in different areas (security threat may not only be external)
- refer to staff action cards to support individual roles during lockdown
- identify staff to man doors and manage any access requirements
- identify staff to inform manager of situation to provide guidance for lockdown
- inform the on call director by telephone. The on call rota and on call director's contact details are in the business continuity folder kept in the post area of reception. The on call director can be contacted via the lynfield mount hospital switchboard on 01274 494194
- inform all staff in the building by email letting them know how often they will receive updates on the situation. Request that staff who are expecting external visitors contact the visitors to alert them of the situation
- contact the emergency services to report the incident and gain advice

Lockdown actions

Communicate lockdown status

- lock all exit / entrance points to the building
- alert on call director for instruction and support
- communicate lockdown to all building occupants via all medium available
- ensure "this is not a drill / practice" is communicated
- keep building occupants updated on the status of the incident

Implement assigned responsibilities

- if required call 999 and request assistance as needed
- start incident log / book
- if riot or malicious individuals outside, close any curtains / blinds / security grills and if safe to do so secure the car park stair gate by the main entrance, stay away from windows and doors

Building occupants

- if riot or malicious individuals outside, close any curtains / blinds, stay away from windows and doors
- if expecting external visitors to the building try to contact them to advise of the situation
- await instructions, updates and or all clear

Recovery

- resume normal operation asap
- ensure any aftercare where required and debriefing are carried out

Appendix 3: Suspicious package and bomb threats procedure

1. Protective measures

The organisation has introduced a number of measures to protect staff when they open post, these include reminders for staff to:

- always open post with letter openers
- keep hands away from noses and mouths
- do not blow into envelopes or shake them
- always wash hands after handling post.

Staff are reminded that there are a number of indications, any of which should alert to the possibility that a letter or package is an explosive device:

- grease marks on the envelope or wrapping
- an odour of marzipan or almonds
- visible wiring or tin foil, especially if the envelope or package is damaged
- the envelope or package may feel very heavy for its size
- if a package, it may have excessive wrapping
- there may be poor handwriting, spelling or typing
- it may be wrongly addressed or come from an unexpected source
- there may be too many stamps for the weight of the package
- it may have been posted somewhere other than Great Britain
- it may have been delivered by hand from an unknown source

Delivered items can include letters, packets and parcels and may contain:

- explosives or incendiary devices
- sharps or blades
- offensive materials
- chemical, biological or radiological (CBR) materials or devices

2. If a suspicious item is found

If a suspicious item is found staff are directed to follow the golden rules:

- do not touch or move
- clear people away from the immediate vicinity
- do not use mobile devices within 15 metres of the suspect package

If a suspicious parcel is found, members of staff should notify the on call director and complete an IR1 form as soon as possible the IR1 form should include details of:

- description of the mail piece (markings, labels, declarations, postage)
- who was the mail addressed to
- what action did you take
- who was the mail received from (internal or external source)

3. Bomb threats

Most bomb threats are made over the phone and the overwhelming majority are hoaxes. Hoax calls can cause alarm and disruption. Any hoax is a crime and must be reported to the police.

Advice on how to handle a threat:

- stay calm and listen
- obtain as much information as possible, try to get the precise location and timing of the alleged bomb and whom they represent. Keep the caller talking
- when the caller rings off, press the directory symbol on your phone. Tab down to received calls to see if you can see the number of the caller
- immediately report the incident to the on call manager who will decide on the best course of action and notify the police
- make notes of your impressions of the caller and an exact account of what was said, these will be needed for the organisations incident reporting procedure and the police

4. Notification and evacuation

4.1. Notification

On discovery of a suspect package or the receipt of a bomb threat the following action must be taken immediately:

- notify the on call director via the lynfield mount hospital switchboard on 01274 494194
- witnesses should complete a BD&C CCG incident report form (IR1) available on the intranet (corporate governance section)

4.2. Evacuation

- the decision to evacuate should be made by the on call director after consultation with others, e.g. police and, if possible, members of the senior leadership team
- the fire alarm will be activated to evacuate the building
- in the event of a decision being made to evacuate, the route taken should be away from the location of the suspect device
- the building must only be reoccupied on the instruction of the on call director

Appendix 4: Increased national threat level procedure

CURRENT THREAT LEVEL		THREAT LEVEL SEVERE TO CRITICAL PARTNERSHIP GUIDANCE Partners should consider the following options as the threat level changes	
SEVERE			
Area Affected		SEVERE "An attack is highly likely"	CRITICAL "An attack is expected imminently"
Process Issue / Governance	Strategic Review Group	Partners to consider convening internal management / governance Group to ensure strategic review of local threat assessment and review local authority response utilising Crisis Management Response Plan (or similar), whilst also dedicating sufficient attention to resource partnership meetings to co-ordinate activity.	Partners to convene internal management / governance Group to ensure strategic review of local threat assessment and review local authority response utilising Crisis Management Response Plan (or similar) whilst also dedicating sufficient attention to resource partnership meetings to co-ordinate activity.
	CONTEST Group	Partners to ensure they have internal CONTEST group covering all aspects of Counter Terrorism. Internal group to be stood up whenever threat level increases.	Internal CONTEST group to be stood up whenever threat level increases.
	Police Liaison	Ensure strong liaison links with local Police Operations and Counter Terrorism leads and Counter Terrorism Liaison Officers.	Contact local force Control Room to confirm current threat assessment and situational awareness to local, regional and national issues that impact on your agency.
	Safety and Security Officer	Identify an individual based at the premises as building safety and security officer (fire and security). Give them a role induction, guidance and time to complete this function. Empower them to escalate identified issues to local authority risk register or equivalent. Partners should ensure they have sufficient contingency around key roles.	Ensure measures in place are implemented.
	Business Continuity Planning	Ensure business continuity plans including invacuation and evacuation drills are up to date and exercised within one month of threat change and at least annually. Ensure building maintenance regime of critical functions and single points of failure (fire and flood) to reduce effect of insider threat sabotage. Prepare and test tannoy messages to brief staff. Identify fall back facilities	Put BCM plans on standby. Make sure all staff are aware of their role.
	Testing / Exercising	Exercise capability to "step-up" and implement options deemed appropriate by Strategic Review Group, ensuring a rolling program of testing and exercising is in place.	Implement options deemed appropriate by Strategic Review Group, ensuring a rolling program of testing and exercising is in place.
	Employment	Review recruitment, vetting and document identification verification policies and processes to ensure insider threat is reduced. Consider Fairway Document Awareness presentation from Police "Fairway Document Awareness.pdf"	Implement actions on recruitment, vetting and document identification verification policies and processes to ensure insider threat is reduced. Consider Fairway Document Awareness presentation from Police "Fairway Document Awareness.pdf"
	Risk Register	Use risk register to record and manage issues, which are beyond the scope of the Governance Group to resolve.	Use risk register to record and manage issues, which are beyond the scope of the Governance Group to resolve.

Staff	Media Strategy	Ensure appropriate communications/ media strategy is in place. Link in with strategic partners to ensure corporate approach where appropriate.	Activate appropriate communications/ media strategy is in place. Link in with strategic partners to ensure corporate approach where appropriate.
	Community Reassurance	Community Reassurance Messaging – assisting with the content, production and delivery of messaging to general and specific community groups depending on the known intelligence at the point the threat level is increased. Liaise with Police Counter Terrorism lead.	Activate Community Reassurance Messaging – assisting with the content, production and delivery of messaging to general and specific community groups depending on the known intelligence at the point the threat level is increased. Liaise with Police Counter Terrorism lead.
	Communications	Consider external and internal communications issues arising from decisions taken by Strategic Review Group. Ensure communication liaison with strategic partners including Police communications.	Consider external and internal communications issues arising from decisions taken by Strategic Review Group. Activate communication liaison with strategic partners including Police communications.
	Deployment	Calls remain unvetted but call handling staff briefed on impact of heightened threat level / Call screening subject to local threat assessment.	Mandated screening / triage of calls prior to deployment of staff
	Call Out Procedures	Ensure call out procedures are tried and tested and contact lists are maintained and up to date.	Activate call out procedures are tried and tested and contact lists are maintained and up to date.
	Strategic Coordination Centres (SCC)	Identify staff that may have a role upon a Strategic Coordination Centre being established and ensure they have knowledge and the support required to carry out their role. Partners should ensure they have sufficient contingency around key roles.	Activate contribution to Strategic Coordination Centre
	Appointments	Staff carry out dynamic risk assessment when attending events / appointments in the public environment and check violent persons register if applicable.	Risk assessment by line manager on all appointments and self-deployment. Consider ceasing non-essential activity in the public environment.

Safety at Work	Training	Review training curriculum in light of threat level. Consider liaison with Police in relation to specific training dependent on threat, e.g. mail handling, bomb threat, Stay Safe, Project Griffin, Project Argus.	Cancellations of all non-essential training ensuring essential services are maintained.
	Corporate Comms / Briefing	Develop a rolling method of re-enforcing safety and security messages (challenge anyone not wearing ID; tailgaters; don't wear ID outside local authority building; hostile reconnaissance awareness. Consider Project Griffin, Project Argus and other presentations available from Police	Activate a rolling method of re-enforcing safety and security messages (challenge anyone not wearing ID; tailgaters; don't wear ID outside local authority building; hostile reconnaissance awareness. Consider Project Griffin, Project Argus and other presentations available from Police. Consider method for advising all staff (including off-duty) of change to critical threat level.
	Corporate Comms / Briefing	Audit staff receipt of threat briefing material including Stay Safe (Run Hide Tell)).	Audit staff receipt of threat briefing material including Stay Safe (Run Hide Tell)
	First Aid Training	Ensure staff training follows current best practice, and reflects outcome of current threat e.g. glass, burns, and firearms attack.	Ensure staff training follows current best practice, and reflects outcome of current threat e.g. glass, burns, and firearms attack.
	Contact Points	Review security arrangements at public contact points.	Close of all non-essential contact points, taking into consideration those points that do not have 'bandit screens' or similar security measures.
	Ongoing Incident	Consider implementing Dynamic Lockdown Procedures in response to a fast moving incident such as a firearms or weapon attack. Ensure such procedures are tested.	Put on standby Dynamic Lockdown in response to a fast moving incident such as a firearms or weapon attack.
	Attendance	Review requirement for non essential staff to attend the workplace Review requirement for essential non patrol staff to wear overtly identifiable uniform / equipment.	Review requirement for non essential staff to attend the workplace Review requirement for essential non patrol staff to wear overtly identifiable uniform / equipment.