Reference Number: *UHB 489* **Version Number:** 03	**Date of Next Review:** January 2029 **Previous Trust/LHB Reference Number:** *Not Applicable – new document*

Corporate Threat Response Procedure

Introduction and Aim

This procedure supports the UHB Security Services Policy and the preparation for "Terrorism – Protection of Premises Act" 2025.

It documents safety and security measures for a considered and proportionate implementation in response to a change in the UK threat level.

Objectives

- Enable CVUHB to minimise known risk and maximise the safety of all employees (including partners), patients and visitors.
- Implement proportionate measures to secure critical assets.
- Support the protection of information and data.

Scope

This procedure applies to all of our staff in all locations including those with honorary contracts

Equality Health Impact Assessment	An Equality Health Impact Assessment (EHIA) has not been completed for this framework – but is considered separately in each of the supporting documents
Documents to read alongside this Procedure	UHB Security Services Policy CVUHB Major Incident Plan CVUHB Business Continuity policy CVUHB Individual service Business Continuity Plans
Approved by	Emergency Preparedness Resilience and Response (EPRR) Strategic Overview Group.

Accountable Executive or Clinical Board Director	Chief Operating Officer.
Author(s)	Head of Emergency Preparedness, Resilience and Response, Head of Security Services.

Summary of reviews/amendments			
Version Number	**Date of Review Approved**	**Date Published**	**Summary of Amendments**
01	05.09.2019	14 October 2021	New document
02	12/07/2023	November 2023	Periodic review – no changes made
03	14/01/2026	15/01/2026	Reference new legislation. “Terrorism – Protection of Premises Act” 2025. Accountable executive updated to Chief Operating Officer.

Content

Appendices

1.0 Overview

1.1 Background

The UK consistently faces a real threat from terrorism, and there remains a serious and sustained threat. The wider impact of this might lead to public disorder, organisational disruption and breaches of security.

In all probability, Cardiff and Vale University Health Board (CVUHB) is more likely to face the challenges of dealing with an individual in dispute with the organisation.

Staff, patient and public safety is a continued priority for CVUHB, and the organisation has established a variety of enhanced security arrangements and operational tactics to ensure that it is both well prepared and protected.

1.2 UK Threat Levels

Since 1970, the UK has had an indicator system used to warn the public of non-specific forms of threat including civil disorder, terrorism or war.

Following the terrorist attacks in London in July 2005, the UK government updated the system which is designed to give a broad indication of the likelihood of a terrorist attack.

The threat level is set nationally based on an assessment by the Joint Terrorist Analysis Centre, using of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities.

There are five threat levels which inform decisions about the level of security required.

UK Threat Levels:

- **Low:** meaning an attack is unlikely
- **Moderate:** meaning an attack is possible, but not likely
- **Substantial:** meaning an attack is a strong possibility
- **Severe:** meaning and attack is highly likely
- **Critical:** meaning and attack is expected imminently

1.3 Aim

In support of the UHB Security Services Policy (Ref: UHB037):

This procedure documents safety and security measures for a considered and proportionate implementation in response to a change in the UK threat level. Further, to support the UHB preparation for the introduction of “Terrorism – Protection of Premises Act” 2025.

1.4 Intentions

It is intended that the procedure will:

- Enable CVUHB to minimise known risk and maximise the safety of all employees (including partners), patients and visitors.
- Implement proportionate measures to secure critical assets.
- Support the protection of information and data.

1.5 Triggers for Activation

This procedure will be utilised in response to:

- An increase in the UK threat level based on intelligence prior to an attack.
- An increase in the UK threat level following an attack on mainland UK or any of its territories.
- A direct/credible threat to CVUHB (even though this may not impact on the UK threat level).
- A decrease in the UK threat level.

2.0 Response

2.1 CVUHB Response Levels

CVUHB has response levels that correspond with the UK threat levels:

National Threat Level	UHB Response Level
Low - an attack is unlikely **Moderate** - an attack is possible but not likely	**Normal**
Substantial - an attack is a strong possibility **Severe** - an attack is highly likely	**Heightened**
Critical - an attack is expected imminently	**Exceptional**

2.2 Normal

CVUHB has a normal operational response level, which is the routine baseline standard for safety and security at its locations. These are the requirements that will be met at all times regardless of the threat level in order to:

- Minimise known risk and maximise the safety of all CVHUB employees (including partners), patients and visitors.
- Secure critical assets.
- Protect information and data.

(See page 07 for full details).

2.3 Heightened and Exceptional

At the heightened and exceptional response levels, additional security measures are required in addition to, and not instead of, the normal response level, and must be incrementally appropriate for each location,

Measures at the heightened level, should be viewed as sustainable indefinitely, whereas those implemented at the exceptional level will only be sustainable for a very limited period.

(See page 09 & 12 for full details).

2.4 Action to Take: Change to the UK Threat Level

In the event of a change to the UK threat level, the Head of EPRR will convene and chair a meeting with representation from:

- Chief Operating Officer
- Director of Capital Estates & Operational Services

- Head of Security
- Clinical & Service Boards
- Communications & Engagement Team
- Police

The group will:

- Assess the risk, implications and relevance to the Health Board.
- Consider whether the situation warrants the implementation of the formal Command, Control and Co-ordination process normally associated with a major incident declaration/business continuity incident. The action cards contained with the major incident plan would be applicable.
- Review the requirements for safety and security at the corresponding response level (sections 2.5, 2.6 & 2.7).
- Agree the measures for implementation.
- Direct the Clinical Board Triumvirates and Directorate Managers/Service Leads to implement the measures, whilst ensuring there is a robust process for reviewing and reporting of effectiveness.
- Agree a communications strategy.

2.5 Response Level: Normal

The baseline standard for safety and security at CVUHB locations when the threat level is low or moderate:

Area	Measures
Minimise Known Risk And Maximise The Safety Of All CVHUB Employees (Including Partners), Patients And Visitors.	
Communications (Situational awareness)	Signage to be displayed inside public areas identifying the need to be vigilant, not to leave bags unattended and that CCTV is operational.
Command & Control	Standard operational management processes.
Security	Standard guard force processes in place. This includes routine patrols, building checks and monitoring of CCTV to identify any response to risks or incidents in a timely manner.
CVHUB employees	Remain vigilant and report any suspicious activity in a timely manner to line managers and Security. Visibly wear staff identification at all times. Never share identification cards or access cards/fobs, and report their loss/theft immediately.
Visitors	Standard operational management processes. No specific restrictions with the exception of standard security, and routine infection, prevention and control guidance.
Patients	Standard operational management processes. No specific restrictions with the exception of standard security, and routine infection, prevention and control guidance.
Secure Critical Assets.	
Buildings & infrastructure	Ensure staff are familiar in securing their areas (setting building alarms, key management etc.). All windows and doors to be secured. Porches, basements, recesses and other areas hidden from immediate view, to be lit at night wherever possible.
Access Control	Never share identification cards or access cards/fobs and report their loss/theft immediately.

Area	Measures
Facilities Management	For clear access/egress routes, areas should be kept free from waste and building access points should be maintained to ensure the safety and security of the building. Repairs affecting site integrity and security to be processed in a timely manner.
Vehicle Access & Parking	All vehicles to be parked in clearly marked designated bays at CVUHB locations. In partnership with the parking operator, enforce parking restrictions. Any vehicle not abiding by this should be asked to move on.
Protect Information And Data.	
Post	Staff receiving and handling post to be vigilant at all times and briefed on the recognition of suspect mail/packages.
Deliveries	Staff receiving and handling deliveries to be vigilant at all times and briefed on the recognition of suspect packages.
IT Systems	All staff to comply with UHB IM&T Security guidance on cyber security - available via the intranet. This would include advice on password management, use of internet, data protection and reporting of suspicious and /or malicious emails.

2.6 Response Level: Heightened

In addition to the baseline standard for safety and security at CVUHB locations, these additional measures must be considered for implementation when the threat level raises to substantial or severe.

Area	Measures
Minimise Known Risk And Maximise The Safety of All CVHUB Employees (Including Partners), Patients And Visitors.	
Communications (Situational awareness)	All staff to be made aware of the heightened response level, and the actions required within CVUHB. **NB.** Scenario-specific messages may be required to support the change in response level.
Command & Control	Standard operational management processes may need to be supplemented by business continuity plans as directed by Clinical Boards, Directorate Managers and Service Leads.
Security	A search and patrol plan of the site to be undertaken and recorded. This should include outbuildings, car parks, yards, basement areas and critical infrastructure buildings. Enhanced presence in public areas, and monitoring of CCTV. Review staff resource which may require enhancement.
CVHUB employees	Challenge (where appropriate) that people have permission to access secure staff areas. Ensure all visitors (for whom they are responsible for) are escorted whilst within secure staff areas.
Visitors	Visitors to be informed via signage or local broadcast media that their baggage should not be left unattended. There may be a requirement to search visitors if they are acting suspiciously. Searching of a person may require police support.
Patients	Patients to be informed via signage or local broadcast media that their baggage should not be left unattended. There may be a requirement to search patients if they are acting suspiciously. Searching of a patient will be carried out following CVUHB procedure, and may require police support.
Secure Critical Assets.	
Buildings & infrastructure	All staff to ensure that faults compromising security are reported to line manager immediately. Line managers are responsible for ensuring that the fault is reported and rectified in a timely manner.

Area	Measures
Access Control	Consider the need to change door lock codes, and restricting access to authorised persons only.
Facilities Management	Regularly check to ensure that all containers which could be used to conceal an explosive device (such as dustbins/crates/boxes etc.) are located in the pre-designated areas. **NB.** All containers must also be regularly emptied. Repairs affecting site integrity and security to be processed as soon as possible.
Vehicle Access & Parking	In partnership with the parking operator restrict and enforce the proximity of parked vehicles, which could be used to conceal explosive devices or block emergency access. Only essential deliveries to be allowed access to areas other than the main stores delivery bays. Only emergency or approved vehicles to be allowed through the security barriers, manned guarding of barriers when required.
Protect Information And Data.	
Post	Consider enhanced surveillance of post received into the UHB. This may result in restricted or delayed delivery. In some instances, the recipient should be asked to attend the post room to validate the items authenticity.
Deliveries	Ensure that all deliveries are made in designated bays/locations. Consider enforcement of pre-agreed delivery timeframes (i.e. Concourse/Transit Stores). Ensure that all 'out of hour' deliveries are communicated to Security Services.
IT Systems	At the point where an attack becomes a strong possibility, consideration for response should include:- • Increase the electronic boundary protection levels on the protection product (to reduce risk of attack). • Block incoming emails. Retain within UHB only capacity. • Prevent internet access – all. However - in the longer term, this will impact remotely accessed (cloud) services but will be an essential protection. • Block access to Remote Desktop Protocol (RDP) and access via Citrix. • Close down patient Wi-Fi and all non-core networks managed within CVUHB.
	Once the attack becomes highly likely, consideration for response should include: - • Begin shutting down non-essential systems based on assessment of threat vector. This may or may not include shared drives.

2.7 Response Level: Exceptional

In addition to the baseline standard, and measures implemented at the heightened response level. These additional measures must be considered for implementation when the threat level is Critical.

Area	Measures
Minimise Known Risk And Maximise The Safety Of All CVHUB Employees (Including Partners), Patients And Visitors.	
Communications (Situational awareness)	All staff to be made aware of the exceptional response level. **NB.** Scenario-specific messages and actions will be required to keep staff, patients & Visitors safe within CVUHB.
Command & Control	Consider whether the situation warrants the implementation of the formal Command, Control and Co-ordination process normally associated with a major incident declaration/business continuity incident. **NB.** This decision will only be made at Executive Director level.
Security	Establish communication link with Police, and UHB Command & Control structure (if established). Increase patrol frequency of critical infrastructure and perimeter locations. Increased regular patrolling of public areas, consider the manned guarding of specific locations (depending on the specific nature of the threat). Continuous monitoring of CCTV required. Further review staff resource which may require enhancement.
CVHUB employees	Follow all instructions from Security staff/Police without question. Ensure all visible door access codes for wards are removed with immediate effect. Never tailgate people (or permit others to) through access-controlled points. In the event of an immediate threat, dial 3333 (or 999 if appropriate).
Visitors	Depending on the nature of the event which has led to 'critical', it may be appropriate to restrict visitors. **NB.** This decision will only be made at Executive Director level.
Patients	Depending on the nature of the event which has led to 'critical', it may be appropriate to restrict admissions. **NB.** This decision will only be made at Executive Director level.
Secure Critical Assets.	
Buildings & infrastructure	Depending on the specific nature of the threat, it may be necessary to instigate lockdown procedures. Report any/all vulnerabilities which affect building integrity and ensure Security Services are aware.

Area	Measures
Access Control	Depending on the specific nature of the threat. Change door lock codes as soon as possible. Restrict access to authorised staff only. Areas to introduce phased security or protection of specific high-risk areas (e.g. Critical Care/Theatres/Paediatrics) when informed to do so.
Facilities Management	Ensure all areas housing services or products which may cause harm are secured, and only accessed by authorised staff stored away. Liaise with Security Services and the Command & Control structure to support the overall response.
Vehicle Access & Parking	Depending on the nature of the event which has led to 'critical', it may be appropriate to severely restrict access to, or even lock down the site. **NB.** This decision will only be made at Executive Director level, and may be in partnership with South Wales Police.
Protect Information And Data.	
Post	Depending on the nature of the event which has led to 'critical', it may be appropriate to restrict postal delivery, distribution and collection to a designated location (i.e. via mail rooms on core sites), where staff will be instructed to decline the delivery. This may preclude independent delivery to some specialist areas - which will again be determined by the nature of the threat and risk to service. **NB.** This decision will only be made at Executive Director level.
Deliveries	Delivery personnel to prove identity and where possible deliver to the main stores loading bays (no deliveries to concourse unless cleared) Departments expecting urgent or essential deliveries to notify Security Services.
IT Systems	Depending on the nature of the event which has led to 'critical', consideration should include:- • Beginning to close network activity to all non-essential functions – i.e. ICT needs to be running to elicit recovery – but most if not all others don't. Need to go through a process of identifying who needs to run – critical roles (from the perspective of recovery and monitoring). • Controlled shutdown of systems that can be shutdown.

2.8 Go Critical

In the event of a direct/credible threat to the CVUHB itself requiring an immediate response at a CVUHB location/s, this specific level of the procedure may be invoked by:-

In-Hours:

- Head of Emergency Preparedness, Resilience and Response
- Head of Security
- Executive Director
- Chief Operating Officer
- Director of Capital Estates & Operational Services

Out of Hours:

- Executive Director / Senior Manager On-Call
- Chief Operating Officer
- Director of Capital Estates & Operational Services
- Security control room

NB. Depending on the nature of the incident, it may also be appropriate/necessary for CVUHB to invoke its Major Incident Plan.

Appendix A

Response Levels (Table Format)

	Normal	Heightened	Exceptional
Minimise known risk and maximise the safety of all CVHUB employees (including partners), patients and visitors.			
Communications (Situational awareness)	Signage to be displayed inside public areas identifying the need to be vigilant, not to leave bags unattended and that CCTV is operational.	All staff to be made aware of the heightened response level, and the actions required within CVUHB. **NB.** Scenario-specific messages may be required to support the change in response level.	All staff to be made aware of the exceptional response level. **NB.** Scenario-specific messages and actions will be required to keep staff, patients & Visitors safe within CVUHB.
Command & Control	Standard operational management processes.	Standard operational management processes may need to be supplemented by business continuity plans as directed by Clinical Boards, Directorate Managers and Service Leads.	Consider whether the situation warrants the implementation of the formal Command, Control and Co-ordination process normally associated with a major incident declaration/business continuity incident.
Security	Standard guard force processes in place. This includes routine patrols, building checks and monitoring of CCTV to identify any response to risks or incidents in a timely manner.	A search and patrol plan of the site to be undertaken and recorded. This should include outbuildings, car parks, yards, basement areas and critical infrastructure buildings. Enhanced presence in public areas and monitoring of CCTV. Review staff resource which may require enhancement.	Establish communication link with Police, and UHB Command & Control structure (if established). Increase patrol frequency of critical infrastructure and perimeter locations. Increased regular patrolling of public areas, consider the manned guarding of specific locations (depending on the specific nature of the threat). Continuous monitoring of CCTV required. Further review staff resource which may require enhancement.

	Normal	Heightened	Exceptional
CVHUB employees	Remain vigilant and report any suspicious activity in a timely manner to line managers and Security. Visibly wear staff identification at all times. Never share identification cards or access cards/fobs and report their loss/theft immediately.	Challenge (where appropriate) that people have permission to access secure staff areas. Ensure all visitors (for whom they are responsible for) are escorted whilst within secure staff areas.	Follow all instructions from Security staff/Police without question. Ensure all visible door access codes for wards are removed with immediate effect. Never tailgate people (or permit others to) through access-controlled points. In the event of an immediate threat, dial 3333 (or 999 if appropriate).
Visitors	Standard operational management processes. No specific restrictions with the exception of standard security, and routine infection, prevention and control guidance.	Visitors to be informed via signage or local broadcast media that their baggage should not be left unattended. There may be a requirement to search visitors if they are acting suspiciously. Searching of a person may require police support.	Depending on the nature of the event which has led to 'critical', it may be appropriate to restrict visitors. **NB.** This decision will only be made at Executive Director level.
Patients	Standard operational management processes. No specific restrictions with the exception of standard security, and routine infection, prevention and control guidance.	Patients to be informed via signage or local broadcast media that their baggage should not be left unattended. There may be a requirement to search patients if they are acting suspiciously. Searching of a patient will be carried out following CVUHB procedure and may require police support.	Depending on the nature of the event which has led to 'critical', it may be appropriate to restrict admissions. **NB.** This decision will only be made at Executive Director level.

	Normal	Heightened	Exceptional
Secure critical assets.			
Buildings & infrastructure	Ensure staff are familiar in securing their areas (setting building alarms, key management etc.). All windows and doors to be secured. Porches, basements, recesses and other areas hidden from immediate view, to be lit at night wherever possible.	All staff to ensure that faults compromising security are reported to line manager immediately. Line managers are responsible for ensuring that the fault is reported and rectified in a timely manner.	Depending on the specific nature of the threat, it may be necessary to instigate lockdown procedures. Report any/all vulnerabilities which affect building integrity and ensure Security Services are aware.
Access Control	Never share identification cards or access cards/fobs and report their loss/theft immediately.	Consider the need to change door lock codes and restricting access to authorised persons only.	Depending on the specific nature of the threat. Change door lock codes as soon as possible. Restrict access to authorised staff only. Areas to introduce phased security or protection of specific high-risk areas (e.g. Critical Care / Theatres / Paediatrics) when informed to do so.
Facilities Management	For clear access/egress routes, areas should be kept free from waste and building access points should be maintained to ensure the safety and security of the building. Repairs affecting site integrity and security to be processed in a timely manner.	Regularly check to ensure that all containers which could be used to conceal an explosive device (such as dustbins / crates / boxes etc.) are located in the pre-designated areas. **NB.** all containers must also be regularly emptied. Repairs affecting site integrity and security to be processed as soon as possible.	Ensure all areas housing services or products which may cause harm are secured and only accessed by authorised staff stored away. Liaise with Security Services and the Command & Control structure to support the overall response.

	Normal	Heightened	Exceptional
Vehicle Access & Parking	All vehicles to be parked in clearly-marked designated bays at CVUHB locations. In partnership with the parking operator, enforce parking restrictions. Any vehicle not abiding by this should be asked to move on.	In partnership with the parking operator restrict and enforce the proximity of parked vehicles, which could be used to conceal explosive devices or block emergency access. Only essential deliveries to be allowed access to areas other than the main stores delivery bays. Only emergency or approved vehicles to be allowed through the security barriers, manned guarding of barriers when required.	Depending on the nature of the event which has led to 'critical', it may be appropriate to severely restrict access to, or even lock down the site. **NB.** This decision will only be made at Executive Director level and may be in partnership with South Wales Police.
Protect information and data.			
Post	Staff receiving and handling post to be vigilant at all times and briefed on the recognition of suspect mail/packages.	Consider enhanced surveillance of post received into the UHB. This may result in restricted or delayed delivery. In some instances, the recipient should be asked to attend the post room to validate the items authenticity.	Depending on the nature of the event which has led to 'critical', it may be appropriate to restrict postal delivery, distribution and collection to a designated location (i.e. via mail rooms on core sites), where staff will be instructed to decline the delivery. This may preclude independent delivery to some specialist areas - which will again be determined by the nature of the threat and risk to service. **NB.** This decision will only be made at Executive Director level.

	Normal	Heightened	Exceptional
Deliveries	Staff receiving and handling deliveries to be vigilant at all times and briefed on the recognition of suspect packages.	Ensure that all deliveries are made in designated bays / locations. Consider enforcement of pre-agreed delivery timeframes (i.e. Concourse/Transit Stores). Ensure that all 'out of hour' deliveries are communicated to Security Services.	Delivery personnel to prove identity and where possible deliver to the main stores loading bays (no deliveries to concourse unless cleared) Departments expecting urgent or essential deliveries to notify Security Services.
IT Systems	All staff to comply with UHB IM&T Security guidance on cyber security - available via the intranet. This would include advice on password management, use of internet, data protection and reporting of suspicious and /or malicious emails.	At the point where an attack becomes a strong possibility, consideration for response should include:- Increase the electronic boundary protection levels on the protection product (to reduce risk of attack). Block incoming emails. Retain within UHB only capacity. Prevent all internet access l. However - in the longer term, this will impact remotely accessed (cloud) services but will be an essential protection. Block access to Remote Desktop Protocol (RDP) and access via Citrix. Close down patient Wi-Fi and all non-core networks managed within CVUHB.	Depending on the nature of the event which has led to 'critical', consideration should include: - Beginning to close network activity to all non-essential functions – i.e. ICT needs to be running to elicit recovery – but most if not all others don't. Need to go through a process of identifying who needs to run – critical roles (from the perspective of recovery and monitoring). Controlled shutdown of systems that can be shutdown.

	Normal	Heightened	Exceptional
		Further consideration for response should include shutting down non-essential systems based on assessment of threat vector. This may or may not include shared drives	