

Victoria Police Manual – Policy Rules

Counter terrorism

Context

Terrorism comprises acts or threats of violence of national concern for the purpose of achieving a political, religious or ideological objective. It may include assassinations, bombings or hostage taking and may endanger critical infrastructure such as public or private buildings, systems or utilities.

Victoria Police is a lead agency in protecting against terrorism or threats of terrorism and managing risk to critical infrastructure. The *Terrorism (Community Protection) Act 2003* (the Act) provides police with a number of special powers to support that role.

These policy rules are intended to further support members in their response to terrorist activity and risk management of critical infrastructure.

Application

Policy Rules are mandatory and provide the minimum standards that employees must apply. Non-compliance with or a departure from a Policy Rule may be subject to management or disciplinary action. Employees must use the Professional and Ethical Standards to inform the decisions they make to support compliance with Policy Rules.

These Policy Rules apply to:

- Operational personnel
- Work Unit Managers
- Criminal investigation Units (CIU)
- Inspectors
- Superintendents
- Security and Organised Crime Intelligence Unit (SOCIU)
- Counter Terrorism Co-ordination Unit (CTCU)
- Regional Emergency Management Inspectors (REMI)
- Critical Infrastructure Protection Unit (CIPU)

Rules and Responsibilities

1. Notification

- Members responding to any incident suspected of being an act or threat of terrorism must immediately notify:
 - Police Communications
 - Security and Organised Crime Intelligence Unit (SOCIU)
 - Serious Crime Desk, Crime Command
- For further guidance on notifications and response, have regard to **VPMG Counter terrorism**.

2. Chemical Biological Radiological (CBR) contamination incident

2.1 *Response*

- Members responding to a CBR incident that has resulted from a terrorist or suspected terrorist act must:
 - cordon and contain the incident scene
 - notify appropriate authority/services via Police Communications.
- For further guidance, consult **VPMG Counter terrorism** and have regard to the **Emergency Response Guide**.

2.2 *Power to detain and decontaminate*

- An Officer must authorise any application of powers under Part 3 of the Act, which provides protection from CBR contamination resulting from a terrorist action or suspected terrorist action, by the detention and decontamination of contaminated persons.
- For further guidance on the application of the power to detain and decontaminate, have regard to **VPMG Counter terrorism**.

2.3 *Theft or loss of prescribed chemicals*

- Attending members must treat all reported losses of quantity of prescribed chemical or substance as a theft and notify CIU of any reported theft/loss.
- CIU must investigate the report
- For further instruction on reporting and investigation responsibilities, have regard to **VPMG Counter terrorism**.

2.4 *Incidents involving Security Sensitive Biological Agents (SSBA's)*

- Refer to the *National Health Security Act 2007* for a list of proscribed SSBA's.

- Attending members must treat all reported incidents involving SSBA's as serious and notify CIU for investigation.
- CIU must notify SOCIU to investigate any possible terrorist links.
- For further instruction on reporting and investigation responsibilities, have regard to **VPMG Counter terrorism**.

3. Preventative Detention Order (PDO)

- A Preventative Detention Order (PDO) under Part 2A of the Act allows for the detention of a person in order to prevent acts of terrorism.
- In the first instance, members considering the use of a PDO, contact the Victoria Police Manager of the Joint Counter Terrorism Team who will liaise with the Work Unit Manager, SOCIU to provide advice and initiate a PDO application, if required.

4. Special Police Powers

- CCP must make application for any authorisation of Special Police Powers (SPPs) under Part 3A of the Act, which provides members with special powers to:
 - protect persons attending events from a terrorist act
 - prevent or reduce the impact of a terrorist act
 - assist in the investigation of or recovery from a terrorist act
 - protect essential services.
- Application process for obtaining SPPs differs depending on the specific purpose. For further information, consult with Special Project Unit and comply with the Act.
- If authorised, the conduct of personal searches under Part 3A must be in accordance with Schedule 1 of the Act and comply with **VPM Searches of a person**.
- Either CTCU or SOCIU must brief members who will be applying the powers on their authority and responsibilities under the Act.
- For further instruction on use of the powers, have regard to **VPMG Counter terrorism**.

5. Critical Infrastructure Protection

5.1 Roles

- Victoria Police have a role under the Act in assisting owners and operators of critical infrastructure that are Declared Essential Services.

- The Critical Infrastructure Protection Unit (CIPU) must coordinate the Victoria Police role in relation to the protection of critical infrastructure, in conjunction with operational police and critical infrastructure owners/operators
- Regional Emergency Management Inspectors have a coordination and monitoring role within their Region
- Station Managers have a liaison, tasking and reporting function within their local areas
- For further instruction on specific roles, have regard to **VPMG Critical infrastructure protection**.

5.2 Information security

- All information and intelligence relating to Critical Infrastructure must be stored according to its security classification, consult **VPMP Information use, handling and storage**.
- Information and intelligence relating to critical infrastructure must not be disclosed to any third party without the written consent of CIPU.

6. Threat Levels and Public Alert Levels

- The Threat Level and Public Alert System are separate and distinct systems. Though threat levels issued by ASIO inform the Public Alert System, the reverse is not the case.
- Threat levels are disseminated by the SOCIU as required. Threat Levels are not public information
- For a more detailed description of the Threat Levels and Public Alert System framework, see the National Counter Terrorism Handbook. Or, for an overview, see the Counter Terrorism Coordination Unit intranet page.

Quick Links

- VPMG Counter terrorism
- VPMG Critical infrastructure protection
- Emergency Response Guide
- *Terrorism (Community Protection) Act 2003*
- *National Health Security Act 2007*

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact your supervisor or the Counter Terrorism Coordination Unit or the Critical Infrastructure Protection Unit.

Update history

Date of first issue	22/02/10	
Date updated	Summary of change	Force File number
24/09/12	Inclusion of instructions about the investigation of SSBA incidents	073168/12
16/01/13	Updated to reflect organisational governance and structural changes.	FF-074790
18/11/13	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
08/04/19	Update to correctly reference VPM Searches of a person	FF-105377