

Victoria Police Manual – Policy Rules

Personnel security

Context

The primary legal source of Victoria Police's information security obligations is the **standards for Victoria Police law enforcement data security (SLEDS)**. The Standards developed by the Commissioner for Privacy and Data Protection outline necessary controls for the secure management of law enforcement data systems and the information they contain. Law enforcement data systems include all relevant data repositories and are not limited to computer systems.

Personnel security includes three major components:

- identification of suitable individuals to access information, resources and assets
- educating Authorised Users about their security responsibilities
- monitoring and evaluation of Authorised Users' continuing suitability.

The security of Victoria Police's people, resources and information is supported by ensuring individuals are subject to pre-employment vetting and personnel security vetting appropriate to the:

- sensitivity and classification of information they need to access
- security classified equipment they use or are responsible for
- valuable resources that they need to access.

This policy provides the Victoria Police rules for the appropriate management of individuals accessing Victoria Police information, resources and assets in line with the Victoria Police Information Management Principles, the six mandatory requirements in the **Australian Government Protective Security Policy Framework (PSPF)** Personnel Security Protocol and the **Information Security Manual**.

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 all Authorised Users.

Rules and Responsibilities

1. Positions requiring Security Clearances

1.1 Requirement

- Authorised Users in positions which require access or are exposed to unclassified information and resources (i.e. below PROTECTED) do not require a security clearance.
- Authorised Users in positions where they are exposed to or responsible for the creation, ongoing use, handling, storage or disposal of security classified information and resources from PROTECTED and above must hold an appropriate security clearance.
- Any other situation where a risk assessment identifies the need for a high level of assurance of an Authorised User's suitability to perform a particular role due to the sensitivity and/or nature of information access, the Authorised User must hold the appropriate level security clearance.
- Victoria Police positions must be assigned as security classified positions if the duties of that position require access to security classified information at the CONFIDENTIAL, SECRET and TOP SECRET level or other situations where the Work Unit Manager determines the need for a high level of assurance of an Authorised User's suitability to perform a particular role.
- Positions that require access to information or resources classified CONFIDENTIAL, SECRET and TOP SECRET are known as Designated Security Assessment Positions (DSAP).
- Authorised Users in a DSAP must hold the appropriate security clearance as set out in the PSPF, Personnel Security Protocol.
- For details on security classification levels and criteria, see **VPMP Information categorisation, collection and recording**.

1.2 Identifying Designated Security Assessment Positions

- Work Unit Managers or authorised officers who have detailed and accurate knowledge of the duties of a position in their work unit must ensure that positions are assessed to determine whether they are Designated Security Assessment Positions (DSAPs).
- Work Unit Managers or authorised officers must ensure that DSAPs within their work unit are periodically reviewed to ensure that the security classification is at the appropriate level.
- The creation of, or variation to, a DSAP must be endorsed by the Work Unit Manager and registered with the Personnel Security Adviser.

- Position Descriptions must include the security clearance requirement appropriate to the level of access.

2. Security clearances

A security clearance is an administrative determination that an Authorised User is eligible and suitable, from a security stand-point, to access security classified resources.

2.1 Requirement

- Authorised User assigned to a DSAP must hold a security clearance at the appropriate level before being granted access to any security classified information or resources.
- The Authorised User's Work Unit Manager or authorised officer must confirm the Authorised User's security clearance status and if required initiate the commencement of the security clearance process using a Request for a Security Clearance [Form 1444]. Refer to **VPMG Security clearances** for more information.
- The responsibility for deciding whether to grant, deny, vary or revoke a security clearance lies with the Agency Security Advisor.

2.2 Adverse Findings

- Vetting decisions are based on an assessment of the whole person and are made in accordance with the Procedural Fairness Guidelines in the PSPF.
- If a security clearance is not granted to the person being assessed (the clearance subject) they are to be provided with details of the reasons and avenues for review of the decision.
- The Work Unit Manager is to ensure that the clearance subject's access to security classified information and/or resources is restricted or limited whilst a review is undertaken.

2.3 Personal Security Files

- Information provided and gathered as part of the security clearance process is only to be used for assessing a person's suitability to hold a security clearance.
- Information collected and created through the security clearance process is to be kept in a Personal Security File.
- The information is to be managed in accordance with the Information Privacy Principles set out in the *Privacy and Data Protection Act 2014* and the PSPF Personnel Security Protocol. This information must not be

released to any person or organization without written consent from the subject of the information, unless there is a legal requirement to do so.

- The Personnel Security Adviser is responsible for storing and controlling access to Personal Security Files.

2.4 *Provisional Security Clearances*

- In exceptional circumstances, where there is an urgent business need for an Authorised User to access security classified information or resources prior to receiving a full security clearance, a provisional security clearance may be considered.
- The Work Unit Manager must seek a provisional security clearance through the Personnel Security Adviser.
- The Work Unit Manager must justify that the business requirement was unforeseen and that the risk to security classified information is outweighed by the urgent business requirement. In making this assessment, they must have regard to **VPMG Security clearances**.

2.5 *Citizenship waivers*

- Only Australian citizens with a checkable background are eligible to be granted a security clearance. Permanent residence status is not an acceptable alternative to the citizenship requirement. If it is necessary for Victoria Police to employ the services of a foreign national in a security classified position, a waiver of the citizenship requirement may be granted in exceptional circumstances by the Chief Commissioner of Police.
- The advantage to Victoria Police must outweigh the potential risks associated with the granting of the waiver. Refer to **VPMG Security clearances** for details of the citizenship waiver process.

2.6 *Limited higher access*

- In exceptional circumstances an Authorised User may be permitted to have access to security classified information at one level above the clearance subject's currently held clearance.
- Limited higher access must be requested by the Authorised User's Work Unit Manager and authorised for a period no longer than three months by the Personnel Security Adviser. Refer to **VPMG Security clearances** for details of process.

2.7 *Recognition of previously issued clearances*

- Current security clearances issued by Australian Government Security Vetting Agency (AGSVA), exempt agencies and States and Territories are to

be recognised by Victoria Police following a review of their Personal Security File and an update of any change of circumstances and basic probity checks.

2.8 Personnel from other agencies

Personnel from other government agencies who are seconded to or co-located with Victoria Police and are required to access security classified information or secure areas, must have an appropriate security clearance. See **VPMG Security clearances** for details.

2.9 Contracted Third Parties and Approved Third Parties

- In accordance with **VPMP Information access**, if CTP or ATP employees access or handle security classified information, an appropriate security clearance must be sought prior to providing access to the information.
- This is to be included in the service level agreement, contract, memorandum of understanding or equivalent agreement.
- The responsibility for and cost of obtaining such clearances for all Authorised Users under the agreement, is to be borne by the CTP or ATP.
- For further information on requirements for CTP or ATP access to Victoria Police information refer to **VPMP Information access**.

2.10 Changes to personal circumstances of security clearance holders

Authorised Users who hold security clearances must report changes in their personal circumstances that may have a bearing on their continued suitability to access security classified information or secure areas. Refer to **VPMG Security clearances** for details of what changes must be reported.

3. Revalidation and review of security clearances

3.1 Requirement

An Authorised Users security clearance must be revalidated as follows:

Assessment	Criteria
Revalidation	• 5 years for Negative vetting level 2 (TOP SECRET) security clearances • 10 years for Negative vetting level 1 (SECRET) security clearances • 15 years for Baseline Vetting (PROTECTED) security clearance • After a significant change in their personal circumstances • If the security clearance level for a Victoria Police position is upgraded • If the security clearance level for a Victoria Police position is downgraded

Assessment	Criteria
Review for cause	• If the Authorised User exhibits changes to behaviour or attitude or intelligence is received that calls into question their suitability to access security classified information • If information is received that the clearance subjects personal circumstances, attitudes or behaviours have changed

Refer to **VPMG Security clearances** for definitions

3.2 **Responsibility**

- The Personnel Security Unit is responsible for the revalidation/review process.
- Authorised Users may be required to provide additional information during the revalidation/review process. The level of information required will be determined by the type of revalidation/review and the level of clearance held by the Authorised User.
- For further details on the process, see **VPMG Security clearances**.

3.3 **Action during review for cause process**

- While a review for cause is being conducted, the Work Unit Manager must determine whether the Authorised User's access to security classified information should be restricted, as informed by the reason for the review, and having regard to **VPMG Security clearances**.

3.4 **Review outcome – clearance to continue**

- If the Personnel Security Adviser is satisfied that the Authorised User's current level of security clearance should continue, they must:
 - inform the Authorised User and their Work Unit Manager
 - continue the clearance, dated from the time of the decision.

3.5 **Review outcome – clearance not to continue**

- If the Personnel Security Adviser is not satisfied that the Authorised User is suitable to maintain their current level of security clearance, they must:
 - immediately notify the Agency Security Advisor who has the delegation to grant, deny, vary or revoke a clearance
 - advise the Authorised User in writing of any downgrade or withdrawal to a security clearance due to a revalidation or review.
- The Authorised User must be given an opportunity to seek a review of the decision.

4. Security incidents

- In accordance with **VPMP Information management and information security framework**, all incidents that breach or may breach the security controls (Personnel, Physical, System or Information Management) must be reported to the Security Incident Registrar (PBEA Protective Security-Security Incident Registry-MGR).
- Work Unit Managers must:
 - report and manage any personnel security incidents occurring in their workplace
 - review the incident and put into place any strategies or practices to prevent future security incidents

Related documents

- VPMG Security clearances
- VPMP Information access
- VPMP Information categorisation, collection and recording

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact the Personnel Security Adviser, Protective Security.

Update history

Date of first issue	22/2/10	
Date updated	Summary of change	Force File number
06/12/10	Inclusion of references to specific CLEDS Standards and name changes of Commonwealth protective security manual to Australian Government protective security policy framework and Information and communication technology security manual to Information security manual.	061979/10
14/02/11	Update of name of the Photo ID and Access Unit	059572/09
18/11/13	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
23/06/14	Complete re-write to align with the National Protective Security Policy Framework (PSPF); CLEDS; Whole of Government initiatives and other regulatory obligations.	FF-085438
15/09/14	Request for a Security Clearance released as VP Form 1444	FF-089469
07/12/15	Legislative reference update to <i>Privacy and Data Protection Act 2014</i> .	FF-096355

25/03/19	Administrative amendments to reflect name change from IMSSD to Protective Security.	FF-139207
----------	---	-----------