

Security clearances

Source Policy

These Procedures and Guidelines support and must be read in conjunction with the following:

- VPMP Personnel security
- VPMP Information categorisation, collection and recording

Application

Procedures and Guidelines are provided to support the interpretation and application of rules and responsibilities. They include recommended good practices and assessment tools to help employees make lawful, ethical and professional decisions. Employees should use the **Professional and ethical standards** to inform the decisions they make to support interpretation of Procedures and Guidelines.

Procedures and Guidelines are not mandatory requirements on their own. However, where rules and responsibilities state that employees must have regard to Procedures and Guidelines, the Procedures and Guidelines must be used to help make decisions in support of the rules.

Procedures and Guidelines

1. General

1.1 Application

- As stated in **VPMP Personnel security**, Authorised Users must hold the appropriate level security clearance when:
 - they are in positions where they are exposed to or responsible for the creation, use, handling, storage and disposal of information or resources classified PROTECTED or above; or
 - the Unit Manager determines the need for a high level of assurance of a person's suitability to perform a particular role is warranted.
- Security vetting, or the security clearance process, is the background checking carried out prior to granting access to sensitive or security classified material or resources.

- Authorised Users do not require a security clearance for ongoing access to unclassified information and resources below PROTECTED.
- The security vetting process is intrusive by its very nature. The process is to be conducted with care and sensitivity as required by the Australian Government Protective Security Policy Framework.
- It is recommended that personnel vetting officers hold a Certificate III in Government (Security) – Personnel Security Stream or equivalent and they have a detailed knowledge of the Personnel Security Core Policy and the requirements outlined in the Protective Security Policy Framework.

1.2 ***Security clearance levels***

There are four security clearance levels, each involving more rigorous checking:

- **Baseline Vetting** – entails screening to permit ongoing access to material classified PROTECTED, or other situations where Victoria Police might determine it needs a higher level of assurance of a person's suitability to perform a particular role.
 - this screening needs to meet the requirements detailed in Australian Standards AS4811:2006-Employment Screening. Victoria Police pre-employment screening does not currently meet the standards outlined in the Australian Standard and is therefore not Baseline Vetting.
- **Negative Vetting Level 1 (NV1)** – a suitability assessment that permits additional ongoing access to CONFIDENTIAL and SECRET resources or other situations where Victoria Police might determine it needs a higher level of assurance of a person's suitability to perform a particular role. This suitability assessment includes Baseline Vetting plus additional suitability checks.
- **Negative Vetting Level 2 (NV2)** – a background investigation that permits additional ongoing access to TOP SECRET resources, or other situation where Victoria Police might determine it needs the highest level of assurance of a person's suitability to perform a particular role. This investigation includes Baseline Vetting plus additional suitability checks as well as background interviews.
- **Positive Vetting** – permits access to resources at all classification levels including certain types of caveated, compartmented and codeword information and usually relates to employment in an Australian Intelligence Community Agency. The Inter-Agency Security Forum on behalf of the Australian Intelligence Community manages positive vetting requirements. It is unlikely Victoria Police personnel will require this level of Security Clearance.

All positions that require access to security classified information or resources above that given by baseline vetting are Designated Security Assessment Positions (DSAPs), as shown below:

Baseline Vetting	Negative Vetting Level 1	Negative Vetting Level 2	Positive vetting
	Designated Security Assessment Positions		

1.3 Access permitted by each clearance level

The following table summarises the access permitted by each clearance level:

		TOP SECRET	SECRET	CONFIDENTIAL	PROTECTED (incl. Sensitive: Cabinet)	Dissemination Limiting Marker & UNCLASSIFIED
CLEARANCE LEVEL	Negative vetting level 2	Yes	Yes	Yes	Yes	Yes
	Negative vetting level 1	NO	Yes	Yes	Yes	Yes
	Baseline vetting	NO	NO	NO	Yes	Yes
Pre-engagement staff screening		NO	NO	NO	Limited access if screened to AS:4811-2006*	Yes

* Limited access is access under supervision to information or resources needed to perform the person's duties for periods not exceeding three months.

- Although a security clearance allows an Authorised User access to classified information, this does not indicate a right-to-know classified information. All access to Victoria Police information is on a need-to-know basis.
- For details on the security classification levels and criteria, see **VPMP Information categorisation, collection and recording**.

2. Determining the need for a Security Clearance

2.1 Identifying a need

- To determine when a security clearance is required, and at what level, the Work Unit Manager should analyse the duties of the position and the highest level of classified information that will be accessed. Refer to

Protective Security Guide F030 How to determine if a Security clearance is required, available from the Protective Security intranet site.

- There are three different situations that may create a need for a security clearance as the role will require access to security classified information. These are a:
 - Victoria Police position (employee)
 - Contracted Third Party or Approved Third Party
 - co-located or seconded Australian Government agency personnel
- In determining the level of security clearance required, the relevant Work Unit Manager should consider the access requirements of the Authorised User to:
 - secure areas
 - Victoria Police files and document storage facilities
 - Victoria Police electronic information holdings.
- Authorised Users accessing classified Information Communication Technology (ICT) networks or systems must have at least the highest level of clearance required to access information that can be held on the network or system. If the ICT networks or systems are compartmentalised the clearance level is that required to access the highest level compartment open to the employee.

2.2 *Victoria Police Position*

- When a position is established, becomes vacant or the existing occupant's security clearance is due for revalidation, the Work Unit Manager should determine what level of security classified information or resources the role is required to access.
- Work Unit Managers should regularly reassess the need for a security clearance of all positions under their control.

2.3 *Contracted Third Parties and Approved Third Parties*

- Contracted Third Parties (CTP) includes any suppliers, contractors, consultants or service providers.
- Approved Third Parties (ATPs) are other government agencies that have been granted direct access to Victoria Police information repositories through their IT system or are periodically sent Victoria Police information.
- When engaging an ATP or CTP, the Work Unit Manager (the Contract Principal or equivalent) must determine the highest level of classified information that will be accessed by the CTP or ATP.

- If this access requires a security clearance, 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**.

2.4 Other Australian Government agency personnel

- There may be occasions where personnel from another Australian Government agency may be co-located in, or seconded to Victoria Police premises.
- Co-location is where Victoria Police shares its office space and/or facilities with another agency.
- Refer to section 8 for details of arrangements for other Australian Government agency personnel.

2.5 Authorised Users clearance

- After determining the need for a security clearance for an employee position, ATP/CTP or other agency personnel, the Work Unit Manager is to confirm the individual's (Authorised User) security clearance status.
- If the Authorised User does not hold an appropriate security clearance for the position, the Work Unit Manager must initiate the security clearance process.
- The Work Unit Manager is accountable and responsible for limiting and monitoring access to security classified information until the appropriate level security clearance is granted.
- Eligibility to hold a security clearance requires Australian citizenship and a checkable background. In exceptional circumstances the eligibility requirement may be waived by the Chief Commissioner of Police in accordance with section 7.

2.6 Recruitment considerations

- Work Unit Managers should appropriately plan recruitment, selection and intended start date to ensure enough time for the completion of the security clearance process.
- Ideally at the time of advertising, the position description should include the requirement for a security clearance, commensurate to the level of

access, if not, notification of this requirement must be prior to making an offer of employment. This will reduce the number of applicants who are unwilling to undergo a clearance applying for the position.

- If an Authorised User, being a VPS employee, is on probation and the required security clearance is not obtained within the initial probation timeframe, probation may be extended for a further three month period to allow finalising the security clearance process. If the application cannot be finalised within that time, refer to provisional access requirements in section 6.

2.7 CTP considerations

- Work Unit Managers should appropriately plan contracting and intended start dates to ensure enough time for the completion of the security clearance process.
- The requirement for a security clearance, matching the level of access required, is to be included where appropriate in procurement documentation.

3. Clearance application process

3.1 Initiation of process

- If an Authorised User does not have an appropriate security clearance, the Work Unit Manager is to initiate the completion of a Request for a Security Clearance [Form 1444] and send it to the Personnel Security Unit (PSU), Information, Systems & Security Command.
- Upon receipt of the Form 1444 by the PSU, the appropriate Security Clearance pack will be emailed to the person being assessed (clearance subject).

3.2 Completion of Security Clearance pack

- The security clearance vetting process can not commence until the completed Security Clearance pack and all supporting documents are received at the Personnel Security Unit.
- Three reminder emails are sent by the PSU to the clearance subject requesting the outstanding security clearance pack.
- The Work Unit Manager is accountable and responsible for an Authorised User ensuring they hold the appropriate level security clearance or undertake the clearance process within three months.
- The Work Unit Manager is accountable and responsible for limiting and monitoring access until the appropriate level security clearance is granted.

- If a person in a position identified as requiring a security clearance fails to comply with the requirement to attain the appropriate level security clearance the Work Unit Manager is accountable and responsible for the level of access granted.

3.3 *Personal Security Files*

- All information relevant to a clearance subject's security vetting is to be maintained in an individual Personal Security File (PSF).
- The Personnel Security Adviser is responsible for storing and controlling access to PSF's.

3.4 *Vetting decisions – assessment of whole person*

- All vetting decisions are based on an assessment of the whole person and at all stages are to be made in accordance with the Australian Government PSPF Procedural Fairness Guidelines.
- In the event that a personal vulnerability emerges in the course of the background assessment the vetting officer is to assess whether any factors exist that mitigate the relevance of the vulnerability.
- The delegation to grant, deny, vary or revoke a security clearance lies with the Agency Security Advisor, Protective Security, Information Systems & Security Command.
- The clearance subject is advised in writing of the decision to grant, continue, deny, revoke or vary a security clearance and any conditions imposed.
- If a security clearance is not granted, the clearance subject is provided with details of the reasons, and the avenues available for review of the decision.
- The clearance subject may respond in writing to the reasons cited. However, this is not possible if the ASIO Security Assessment is unfavourable.

3.5 *Favourable findings*

- When a clearance is granted, the clearance subject is provided with either a security awareness briefing or documents that clearly detail the clearance holder's responsibilities, including the need to report any change of personal circumstances.
- The clearance subject is required to sign the security clearance notification form acknowledging receipt of having read and understood the roles and responsibilities of holding a security clearance.

- Work Unit Managers are to ensure that the clearance holder understands and accepts their day to day security responsibilities.

3.6 *Adverse findings*

- If the Personnel Security Advisor is satisfied that the clearance subject is not suitable to be granted or continue to hold their level of security clearance, the Personnel Security Advisor is to:
 - advise the delegate in writing of reasons for the clearance subject not being suitable
 - if the clearance subject is within the probationary period during which time a security clearance is to be attained, notify Employee Relations, Human Resource Department for advice on the dismissal process
 - notify the Work Unit Manager of potential adverse findings to ensure that the clearance subject's access to sensitive or classified information and/or resources is restricted pending the final decision by the delegate
 - advise the clearance subject of the concerns and give them an opportunity to respond in writing
 - forward the Authorised User's response along with the Personnel Security Advisor's recommendation to the delegate for a decision.
- The recommendation by the delegate can range from (but is not limited to):
 - if on probation in a DSAP dismiss the employee
 - if under contract, direct the removal of the individual (in accordance with **VPMP Information management and information security framework**)
 - withdrawing or denying the security clearance
 - downgrading the security clearance
 - applying conditions to the security clearance.
- The clearance subject is to be advised in writing of the decision and procedures for seeking a review of the decision.

3.7 *Uncheckable background*

- A clearance subject has an uncheckable background if the Personnel Security Unit (PSU) cannot complete the minimum checks and inquires for the level required.
- If the clearance subject has an uncheckable background the process as detailed in 3.6 is to be followed.

4. Ongoing management (Aftercare)

4.1 Overview

- The initial security vetting process only provides a snapshot of an individual at a particular time.
- Periodic revalidations of the security clearance must occur in accordance with **VPMP Personnel security**.
- Clearance holders are responsible for notifying PSU of any significant change in circumstances.
- Command and Work Unit Managers are responsible for providing support, awareness and education as part of the aftercare regime.
- The Personnel Security Unit as a minimum will provide security awareness training as part of a revalidation process.

4.2 Criteria for revalidation or review

An Authorised User's 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
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

4.3 Responsibilities

- The Personnel Security Unit is responsible for initiating and conducting 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.

4.4 Outcomes from revalidation or review

- If the Personnel Security Adviser is satisfied that the Authorised User should continue having the current level of security clearance, they will:
 - inform the Authorised User and their Work Unit Manager
 - continue the clearance, dated from the time of the decision.
- If the Personnel Security Adviser is not satisfied that the current level of security clearance should continue they will submit a report in writing to the Agency Security Advisor in line with section 3.6.
- The Authorised User should be given an opportunity to respond in writing to the concerns raised which should accompany the Personnel Security Adviser's recommendation to the Agency Security Advisor.
- The Personnel Security Adviser may recommend actions including but not limited to:
 - reminding the subject of their responsibilities
 - reallocating duties to other staff
 - prohibiting after-hours entry
 - restricting access to security containers or IT systems
 - close supervision of the employee
 - withdrawing the clearance
 - aftercare provisions.

4.5 Change in circumstances reporting requirements

- Changes in circumstances may impact on the clearance holder's continued suitability to hold a security clearance.
- Clearance holders are to advise the PSU of any changes in personal circumstances.
- Changes to personal circumstance are to be reported as soon as practicable after the change occurs. Work Unit Managers are to ensure that clearance holders report these changes.
- Work Unit Managers should also report any changes in circumstance relating to clearance holders if they become aware of these changes and are unsure whether the changes have been notified by the clearance holder.
- All clearance holders should also report significant changes in circumstance in other individuals where they feel it may impact on security.

4.6 *Type of personal circumstances changes*

- Clearance holders are to report the following changes in circumstance:
 - entering into, or ceasing, a marriage or domestic partnership
 - visits to, or residence in, foreign countries (official or private travel – see section 5.3)
 - change of residential/permanent address
 - relatives residing in foreign countries of security significance
 - breaches of the Code of Conduct
 - changes in citizenship or nationality
 - non-routine communications with employees of any foreign government
 - changes in financial circumstances only if significant – e.g., credit refusal, bankruptcy, gambling or other debts causing financial hardship
 - involvement in criminal activity including traffic offences (and any pending matters)
 - involvement with any individual, group, society or organisation that may be of security concern
 - subject to a discipline or criminal investigation, or a complaint submitted to PSC
 - subject of Security Incident
 - name change
 - persons (over 18) residing with you
 - commenced any secondary employment
 - any other changes in circumstances that may be of concern
- Documentary evidence must be provided in support of any of the above changes as required by **VPMP Personnel security** and will be attached to the Personal Security File
- A Change of Circumstances form is available from the Personnel Security Unit to address any changes.

4.7 *Reporting overseas travel*

When a clearance holder undertakes official overseas travel, they are to advise the Personnel Security Adviser in writing. The Personnel Security Adviser will update the clearance holder's PSF with this information, and if required:

- provide a security travel briefing to the clearance holder based on the DFAT Smartraveller Advisory Service.

Before a clearance holder undertakes private overseas travel, they are to notify the Personnel Security Adviser in writing. The Personnel Security Adviser will:

- update the clearance holder's PSF with this information, and if requested by the security clearance holder may:

- provide a security travel briefing to the clearance holder based on the DFAT Smartraveller Advisory Service.

4.8 Clearance subject leaves the agency

- When a clearance subject leaves Victoria Police, the security clearance becomes inactive.
- The PSF will be forwarded to the Australian Government Security Vetting Agency (AGSVA) or another agency upon receipt of a signed 'Consent to release PSF' form.
- Prior to transfer of the PSF, any agency specific checks or other third party information with the understanding of confidentiality that was provided specifically to Victoria Police will be removed.
- The physical transfer of the PSF is to be in accordance with **VPMP Information use, handling and storage**.

4.9 Disposal of PSFs

Disposal of PSFs must be in accordance with **VPMP Information review, retention and disposal**.

5. Review of processes and outcomes

5.1 Request for review

If a clearance subject feels aggrieved by either the security clearance process or the security clearance decision a written report outlining the issues or concerns should be forwarded the Agency Security Advisor.

5.2 Action during the review period

- As required by **VPMP Personnel security**, Work Unit Managers must determine whether the Authorised User's access to sensitive or classified information and/or resources should be restricted, as informed by the reason for the review.
- The Authorised User should be treated like any other person who is unable to fulfil the duties of their position. No measures should be applied that would have a negative impact on the Authorised User beyond those necessary for the maintenance of effective protective security.
- Only in the most extreme case should the Victoria Police employee be denied access to their work area. This is particularly important where a review for cause process is triggered by information or an event of security significance involving the employee.

- Decisions and actions taken during this period could be subject to review by the courts. Victoria Police must be able to demonstrate that the requirements of natural justice were met.
- Before taking any adverse action against the employee, Victoria Police should ensure that information contained on the Personal Security File is current and if that information is relevant to the proposed action.

6. Temporary access

There are three types of temporary access arrangements. They are:

Access to	Type of access		
	Limited higher access (Maximum period 3 months)	Emergency or short term access (Maximum period 3 months)	Provisional access (Access until clearance process is finalised)
TOP SECRET	Contact Personnel Security Advisor for approval	Contact Personnel Security Advisor for approval	Can be approved by Victoria Police Agency Security Advisor
SECRET and below	Can be approved by Victoria Police Agency Security Advisor	Can be approved by Victoria Police Agency Security Advisor	Can be approved by Victoria Police Agency Security Advisor

Conditions for their use are explained below.

6.1 Limited Higher access

- The Victoria Police Agency Security Advisor may approve limited higher access to material up to and including SECRET for individuals providing the access is both:
 - limited to one level higher than the currently held clearance
 - for less than three months.
- Work Unit Managers are to forward formal written advice, including justification for the limited higher access to the Personnel Security Advisor.
- The Work Unit Manager is to strictly control the Authorised User's access to information relating to the project or issue on the 'need to know' principle.
- If the Work Unit Manager expects that there will be an ongoing need to access higher level material the security clearance level is to be formally upgraded and a request for an upgrade is to be submitted.

6.2 *Emergency or one-off short term access*

- The Agency Security Advisor may approve emergency access to material up to and including SECRET to meet an immediate and critical requirement.
- Emergency access may be approved to an Authorised User where they do not have the appropriate clearance and cannot be given access under the provisions of limited higher access.
- An emergency access clearance can not be considered until the clearance subject submits the relevant level security pack with the supporting documents.
- The clearance package will be assessed and approval recommended for emergency access.
- The decision to approve emergency access constitutes an increased risk of compromise therefore a risk assessment is to be carried out and consultation with any affected external agency prior to granting approval.
- Emergency access to security classified resources may only be approved when:
 - The Authorised User needs immediate access for their role
 - The access is to cover a specific situation not exceeding three months' duration
 - The Authorised User only has access to essential information
 - The Authorised User's access is appropriately supervised
 - The Authorised User receives a security briefing
 - The Authorised User signs an undertaking to protect official information
- A record of the approval of the emergency access is maintained at the Personnel Security Unit including the reasons for the access and details of the Authorised User.

6.3 *Provisional access*

- In exceptional circumstances and where there is an urgent business need, an Authorised User may be eligible for a provisional security clearance prior to being granted a full security clearance.
- A provisional clearance can not be considered until the clearance subject submits the relevant level security pack with the supporting documents.
- The Personnel Security Unit will review requests for provisional access within fourteen days of receipt of the completed clearance pack.
- In accordance with **VPMP Personnel security**, before approving provisional access, the Agency Security Advisor must be satisfied there are no obvious indicators suggesting the security clearance may be problematic or that

may bring into question the clearance subject's general suitability to hold a security clearance.

- Provisional access will continue until the clearance process is finalised unless there are any identified concerns relating to the clearance subject's suitability.
- A provisional security clearance may be granted when all other checks and processes are complete even if ASIO is outstanding.
- Any emergency or limited higher accesses are to be the exception and are not to be used to replace the security clearance process.

7. Australian Citizenship requirements

7.1 *Citizenship Waiver Process*

If Victoria Police engages a non-Australian citizen in a security classified position, in exceptional circumstances, a waiver of the citizenship requirement may be granted by the Chief Commissioner of Police.

- The citizenship waiver process will not ordinarily be undertaken in cases where an Australian citizen could fulfil the requirements of the position.
- The granting of a citizenship waiver is separate to the security clearance process.
- Completion of the waiver application followed by the security clearance process may take two months or longer to complete.
 - Work Unit Managers should therefore start recruiting or contracting at least two months prior to the intended start date to ensure enough time for the completion of these processes.
- Non-Australian citizens must hold the appropriate working visa before a citizenship waiver request is considered.
 - the Work Unit Manager sponsoring the Non-Australian is to verify that they hold an appropriate working visa.

The Work Unit Manager is to prepare and forward a written report to the Personnel Security Advisor. The report should include:

- request for consideration for a citizenship waiver
- a work area security risk assessment, including mitigations and any residual risks identified
- details of the exceptional circumstances including:
 - the specialist skills required by not available from a suitable person who would otherwise be eligible for a clearance and

- why the duties cannot be redesigned so that the classified information or resources only needs to be accessed by security cleared employees
- consideration of the residency status and citizenship intentions of the Non-Australian citizen.
- The report is forwarded in hard copy to the Personnel Security Adviser who will seek security intelligence advice on the country of citizenship before applying for a citizenship waiver for a national security clearance.
 - written advice from ASIO should be part of the submission.
- The Personnel Security Adviser is to advise in writing any third parties that may be affected by the granting of the waiver.
- The Personnel Security Adviser will prepare a submission for the Chief Commissioner to determine whether to grant the waiver.

7.2 Security clearance application (Citizenship Waiver)

- The security clearance process should be conducted concurrently with a citizenship waiver but is not to be completed until the waiver is granted.
- The citizenship waiver does not pre-empt the security clearance process.
- If the citizenship waiver is not granted the security clearance process will be cancelled.
- A Non-Australian citizen granted a security clearance is to be informed that his or her security clearance is only valid whilst employed with Victoria Police.
- The Personnel Security Advisor should monitor any conditions placed on a citizenship waiver as part of the clearance aftercare process.
- A citizenship waiver will be reassessed at least every two years by the Personnel Security Advisor.

7.3 Certificate of Suitability

- The PSPF guidelines require Australian citizenship for eligibility to hold a security clearance.
- However, as Victoria Police does not have a requirement for employees to hold Australian citizenship, a Non Australian may be granted a Certificate of Suitability as an alternative. The same vetting processes are undertaken except for the ASIO assessment.
- A Certificate of Suitability granted to a non citizen is relevant only whilst employed at Victoria Police and is not be transferrable to any other agency.

- Non- Australian citizens granted a Certificate of Suitability are not to be given access to security classified resources originating from a third country unless that country has specifically approved their release in accordance with bilateral agreements.
- A Certificate of Suitability can provide the same level of access to information and secure areas as does a security clearance, having regard to the restrictions on intelligence resources originating from third countries.
- The Certificate of Suitability can be upgraded to Negative Vetting level 1 or Negative Vetting level 2 when Australian citizenship is received.
- Certificate of Suitability will be reviewed by the Personnel Security Advisor at least every two years.

7.4 Recording

All citizenship waiver requests and subsequent decisions are documented in the Personnel Security Unit Register kept by the Personnel Security Adviser.

8. Personnel from other agencies

8.1 General requirements regarding secondments

- The Australian Government Security Vetting Agency (AGSVA), exempt agencies and States and Territories are to recognise each other's clearances unless one of the following conditions exist:
 - the clearance has lapsed
 - the clearance was granted based on an eligibility waiver
 - AGSVA or an exempt agency has substantial prejudicial information that the incoming employee is no longer suitable to access security classified information at the required level.
- The Personnel Security Unit will address any anomalies within the incoming employee's Personal Security File at the time of transfer.
- The security requirements for personnel seconded to Victoria Police are:

If the seconded person ...	Then ...
Does not have a security clearance	Victoria Police will conduct a security clearance at the level required
Has a lower level clearance than that required	The clearance subject's agency should provide Victoria Police with a copy of the Personal Security File to enable the Personnel Security Unit to upgrade the clearance to the appropriate level.

If the seconded person ...	Then ...
Is already cleared to the appropriate level, or a higher level than required	Victoria Police will seek confirmation of: - the level of clearance - the date the clearance was granted and date it will expire - whether the clearance is conditional upon any aftercare arrangements.

8.2 Conditions

If the seconded person's clearance lapses during the course of the secondment period, renewal of the clearance is the responsibility of the out-posting agency.

Further Advice and Information

For further advice and assistance regarding these Procedures and Guidelines, contact the Personnel Security Adviser.

Update history

Date of first issue	22/2/10	
Date updated	Summary of change	Force File number
18/11/13	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
23/6/14	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
25/03/19	Administrative amendment to reflect name change from IMSSD to Protective Security.	FF-139207