

Victoria Police Manual

The Victoria Police Manual is issued under the authority of the Chief Commissioner of Police in s.60, Victoria Police Act 2013. Non-compliance with or a departure from the Victoria Police Manual may be subject to management or disciplinary action. Employees must use VPM Professional and ethical standards to inform the decisions they make to support compliance.

Service provider and external personnel security requirements

Context

Victoria Police is required to adhere to the [Victorian Protective Data Security Standards \(VPDSS\)](#) issued by the Office of the Victorian Information Commissioner. The standards require protective security to be embedded in contracted service provider arrangements, which should align with the Australian Government Protective Security Police Framework (PSPF).

This policy supports Victoria Police's compliance with the VPDSS standards and the PSPF and is informed by the Victoria Police Protective Data Security Plan.

Contents

Context.....	1
Contents.....	1
Definitions.....	1
Scope and application.....	2
Policy.....	2
Responsibilities and procedures	2
1. Procurement.....	2
2. Security check requirements.....	2
3. Access to security classified information	6
4. Additional access to facilities (beyond the initial engagement)	6
5. Victoria Police Photo Identification Cards.....	6
6. LEAP flags – service providers and external government personnel.....	7
7. LEDR MK2 – external non-government personnel (VPC occupants)	8
8. Contact with police outside of role of employment	8
9. Assessment of suitability following contact with police.....	8
10. End of service or termination process.....	9
Further advice and information.....	9
Update history.....	9

Definitions

External government agency personnel – is an employee of an Australian State/Territory, or Federal Government agency whose permanent place of work is the Victoria Police Centre (VPC), or who requires access to Victoria Police facilities to undertake their duties.

External non-government personnel – is an employee of an organisation whose permanent place of work is the VPC (e.g. BankVic VPC Branch, Neighbourhood Watch). This does not include service providers as defined below.

Law Enforcement Assistance Program (LEAP) - is the main central system used to record details of incidents, crimes, people and locations in support of operational policing activities.

LEDR MK2 - is a functionality within LEAP which allows for the recording of 'Field Contacts'.

Security classified information – is any information with a protective marking of PROTECTED, SECRET or TOP SECRET.

Service provider – is a contractor, consultant or other person who is or has been engaged to

provide services to Victoria Police or to the Chief Commissioner of Police; or a person who is or has been employed by or engaged to provide services to an external government agency, external non-government agency or other service provider located within a Victoria Police facility.

Victoria Police information – is information, documentation and data in any form, including ‘Law Enforcement Data’ which is created, obtained, received, stored or released by Victoria Police (or individuals in the course of their duties as employees of Victoria Police) for any of the functions or activities of Victoria Police.

Scope and application

This policy applies to all Victoria Police employees, service providers, external government agency personnel and external non-government personnel requiring access to Victoria Police information, equipment, systems and/or unescorted access to Victoria Police facilities.

Policy

To access Victoria Police facilities, information, equipment, and systems all service providers, external government agency and non-government personnel (external personnel) must be subjected to personnel security checks as set out in this policy.

Service providers and external personnel accessing Victoria Police information, equipment, systems and/or facilities must comply with their contract and/or the Deed of Contract (Contractor Security Check) regarding information and equipment management and security.

Responsibilities and procedures

1. Procurement

- When procuring goods or services, work unit managers must identify and mitigate security risks to Victoria Police employees and service providers, information, and assets. At a minimum, personnel security checks must be completed.
- Standard contracts must include relevant security terms and conditions which apply appropriate information, physical, and personnel security requirements under the VPDSS and the PSPF.

2. Security check requirements

2.1 *Service providers and external government agency personnel who require access to Victoria Police facilities*

- A Victoria Police Contractor Security Check must be completed for all service providers or external government agency personnel who have a legitimate business need and require access to Victoria Police facilities.
- The CSU, SIPD is responsible for conducting the Contractor Security Check to determine suitability (refer to section 2.4 of this policy).
- An online e-pack application for the Contractor Security Check can be obtained directly from the CSU.
- The cost of undertaking the security checks and procuring any necessary security clearances is the responsibility of the service provider or external government agency.

- Victoria Police facilities must only be accessed once the check has been completed and the individual has been deemed suitable by the CSU.
- A Victoria Police issued Photo Identification Card will be provided.
- Service providers and external government agency personnel are not permitted entry to a secured area without the required checks completed and the relevant Victoria Police issued Photo Identification Card, which must be displayed on the approved lanyard.

2.2 *Service providers and external government agency personnel who require access to Victoria Police information and/or systems*

- A Victoria Police Contractor Security Check must be completed for all service providers and external government agency personnel who require access to Victoria Police information and/or systems for a legitimate business need.
- The CSU, SIPD is responsible for conducting the Contractor Security Check to determine suitability (refer to section 2.4 of this policy).
- The cost of undertaking the security checks and procuring any necessary security clearances is the responsibility of the service provider or external government agency.
- Where a service provider requires access to Victoria Police information, a written agreement must be in place within the terms of their engagement arrangement, in addition to the Victoria Police Contractor Security Check.
- A Victoria Police issued Photo Identification Card will be provided.
- Victoria Police information and/or systems must only be accessed once the check has been completed and the individual has been deemed suitable by the CSU and provided with the relevant information management policies.

2.3 *External non-government personnel who require access to the VPC*

- A Victoria Police Contractor Security Check must be completed for all external non-government personnel who have a legitimate business need and require access to the VPC.
- The CSU, SIPD is responsible for conducting the Contractor Security Check to determine suitability (refer to section 2.4 of this policy).
- An online e-pack application for the Contractor Security Check can be obtained directly from the CSU.
- A Victoria Police issued Photo Identification Card will be provided.
- The VPC must only be accessed once the check has been completed and the individual has been deemed suitable by the CSU.

2.4 *Security checks*

- The CSU is responsible for administering security checks and ensuring that checks have been completed in full.
- Security checks do not involve an assessment of the individual's character and are not considered a security clearance. As such, the individual who is the subject of the security checks should not be asked to disclose additional information about their background.

- All information and documentation relating to security checks must be retained in accordance with F140 *Common Administrative Records Retention Factsheet*.
- The service provider or external personnel must undergo the following security checks:

Security Checks	Primary Purpose of Security Check
Validation of identity documents through the Document Verification Service. Identity verification must be to Level of Assurance Three as defined in the Australian Government National Identity Proofing Guidelines.	To: • establish confidence in the person's identity • mitigate against the risk of fraud against Victoria Police • mitigate the unauthorised access to and disclosure of sensitive information.
Police Name Check (for access to facilities) or Police Name and Fingerprint Check (for access to information and/or systems). Interstate individuals must also undergo a National Police Name Check from an accredited body or Australian police agency within the last three months, or a check on LEAP National Police Reference System.	To: • mitigate the risk of theft, damage or sabotage to Victoria Police assets and information • mitigate the unauthorised access to and disclosure of sensitive information • for fingerprint checks, identify if the individual has a criminal history and has changed their identity.
Verification of any foreign national's visa details and conditions through the Department of Home Affairs Visa Entitlement Verification Online (VEVO).	To verify that the individual has an entitlement to work in Australia.
Overseas Police Check of any foreign nationals residing in Australia for less than five years. The police check or checks from the country of origin and, any subsequent countries of residence within those five years must be obtained. For individuals based overseas, a Police Check from the current country of residence and any other countries of residence over the previous five years must be obtained. International police checks must be translated by a National Accreditation Authority for Translators and Interpreters (NAATI) accredited translator and certified.	To: • verify that an individual has no criminal history overseas • mitigate against the risk of fraud against Victoria Police • mitigate the unauthorised access and disclosure of sensitive information.
Review of Victoria Police intelligence holdings.	To:

	• identify if the individual is subject to any current investigations • identify if the individual is involved with any non-declared criminal associations which may not be evident through LEAP.
Deed of Confidentiality	To protect against disclosure of confidential information, intellectual property, and other confidential information.
Declarable Association Declaration	To identify and assess individuals with associations to persons or groups who have the intent and capability to adversely impact Victoria Police capability, impede an investigation or facilitate a serious offence.
Conflict of interest declaration	To identify and assess any actual, potential or perceived conflict of interest that may give rise to actual or potential financial gain.

2.5 Assessment of security checks

- Generally, CSU will make a determination regarding an individual with no criminal record or involvement.
- For individuals with a criminal record or involvement, the Security Operations Manager, SIPD, or their nominated delegate is responsible for determining their suitability.
- The Security Operations Manager, SIPD or their nominated delegate should assess service providers or external government personnel who have a disclosable court outcome on a case-by-case basis and, consider the relevance of the offence against the primary purpose of the security check. The following table should be used as a guideline for assessing such matters:

Key Criteria	Risk Tolerance
The date of the offence(s) and conviction	The assessor should not consider spent convictions.
Age of the individual at the time of the offence(s) or conduct.	The assessor should not consider offence(s) or conduct where the individual was a juvenile, unless the length of time since the offence was less than 5 years and the offence was a serious offence.
Seriousness of the offence(s) or conduct	The following offence(s) are considered serious, and should preclude an individual from being given ongoing and/or unsupervised access to Victoria Police facilities and/or information: • a serious indictable offence as defined under s.325(6) <i>Crimes Act 1958</i> • offence for assault, hinder, obstruct or resist a police officer or any other public official • violent or sexual offences

	- family violence offences (including property crime) and stalking - dishonesty offences, including theft, fraud, obtaining benefit by deception, forgery, impersonation, and false or misleading information - corruption activities or related offences - drug related offences - firearm or weapon related offences - the individual is subject of a current and or outstanding arrest warrant or intervention order - the individual is or has been a registrable offender under the <i>Sex Offender Registration Act 2004</i>.
Frequency or repeated nature of the offence(s) or conduct	Where an individual has three or more non-serious offences, the assessor should consider the length of time since the offence occurred in determining whether the matter should preclude an individual from being given ongoing and/or unsupervised access to Victoria Police facilities and/or information.

- Individuals should be afforded an opportunity to explain the circumstances surrounding any criminal record prior to a determination being made.
- Where an individual seeks a review of an unfavourable outcome, the matter should be referred to the Superintendent, SIPD for review.

3. Access to security classified information

- Where a service provider is required to access Security Classified Information, a National Security Clearance will be required. If undertaking system administrative functions, usually a clearance one level higher than the information to be accessed is required.
- Guidance on obtaining a National Security Clearance is contained in Factsheet 045.

4. Additional access to facilities (beyond the initial engagement)

If the service provider or external personnel require additional access to facilities other than those included in the initial engagement, access must be approved in writing by the Officer in Charge (OIC) of that facility or their authorised delegate.

5. Victoria Police Photo Identification Cards

5.1 General

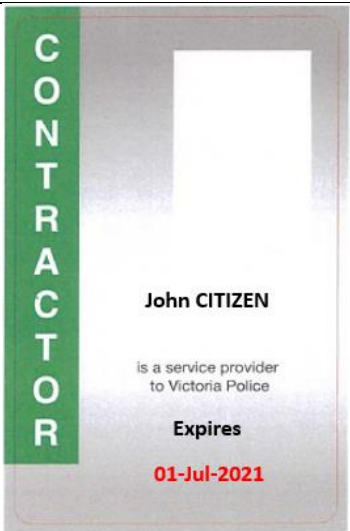
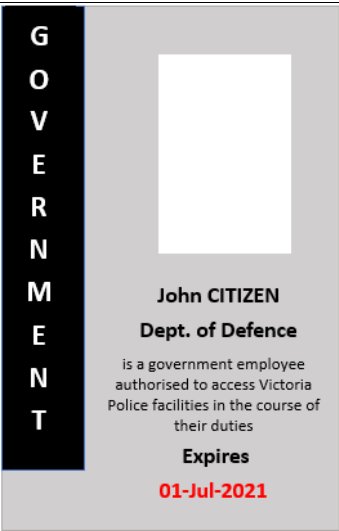
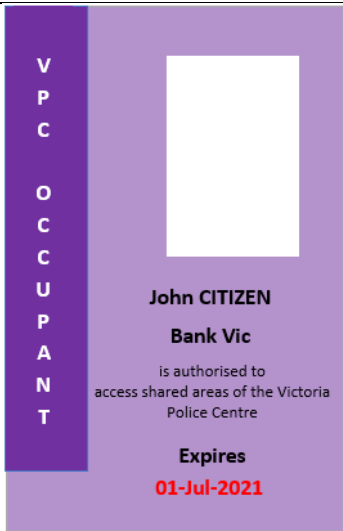
- The CSU is responsible for issuing Victoria Police Photo Identification Cards and lanyards as per section 5.3 of this policy.
- VPC Precinct Services must direct enquiries relating to expired Photo Identification Cards to the CSU.

5.2 Urgent works – additional requirements

- To allow for urgent works to be undertaken prior to the individual's receipt of the Victoria Police Contractor Photo Identification Card, a Service Provider Approval Notice will be issued to the individual by CSU, and a copy will be issued to the Victoria Police nominated representative detailed on the e-pack application (the relevant contract manager).
- The OIC of the relevant Victoria Police Facility (or their delegate) must validate the identity of the individual on presentation of the Service Provider Approval Notice (using government issued photo identification such as driver's license).

5.3 Types of Victoria Police Photo Identification Cards

- The below images reflect the different types of identification cards issued to service providers and external personnel.
- Where issued these cards must be displayed with the correct lanyard when attending any Victoria Police facility.

Service provider	External Government Agency Personnel	External, Non-Government Personnel
		
Orange Lanyard (Properties) Green Lanyard (Consultant)	Black Lanyard	Purple Lanyard

6. LEAP flags – service providers and external government agency personnel

- Once service providers or external government agency personnel have been approved for engagement at Victoria Police, the CSU must create an 'Interest Flag' against their profile on LEAP.
- The 'Interest Flag' is displayed on the 'Master Name Summary' screen and should be recorded as 'Victoria Police – Contractor'.
- The flag should be marked as 'active' to indicate that the service provider or external government agency personnel's status is current and valid.

7. LEDR MK2 – external non-government personnel (VPC occupants)

- Once external non-government personnel have been approved for access to shared spaces within the VPC, CSU must enter a 'Field Contact' against the individual's profile within LEDR MK2.
- Attached to this 'Field Contact' function is a 'Remarks and Additional Information' section which details a set of instructions.
- The field contact should be marked as 'active' to indicate that the external non-government personnel's status is current and valid.

8. Contact with police outside of role of employment

- If members come into contact with an individual who is flagged on LEAP as "Victoria Police – Contractor", members must check the 'Remarks' section of the interest flag on LEAP and ensure the instructions are followed.
- If members come into contact with an individual who is noted in LEDR MK2 as a VPC occupant, members must check the 'Additional Information' within the 'Field Contact' and ensure the instructions are followed.
- Members must notify SIPD as soon as is practicable via either:
 - CONTRACTOR-SECURITY-MGR@police.vic.gov.au
 - PHYSICAL SECURITY-MGR@police.vic.gov.au
 - SECURITY INCIDENTS-MGR@police.vic.gov.au.

9. Assessment of suitability following contact with police

- Where notified as per section 8 of this policy, the CSU must, as soon as practicable following notification, conduct a further assessment of the individual's suitability to continue their access to Victoria Police facilities, systems and/or information using the guidelines provided in section 2.5 of this policy.
- The Security Operations Manager, SIPD, or their nominated delegate is responsible for deciding whether it is suitable for an individual to continue their access to Victoria Police facilities, systems and/or information.
- Where an individual seeks a review of an unfavourable assessment, the matter should be referred to the Superintendent, SIPD for review and final determination.
- If a service provider is assessed as posing a security risk to Victoria Police, CSU will issue an instruction to the nominated organisation's point of contact that the individual is to be removed from any agreement for service provision to Victoria Police or authorisation to work within the VPC, via either:
 - for service providers and external government agency personnel, the relevant Victoria Police contract manager
 - for external non-government personnel, the Victoria Police Properties Division (Leasing and Accommodation).
- CSU in consultation with relevant work areas is responsible for ensuring that access to Victoria Police facilities and systems is immediately removed and that any Victoria Police Photo Identification Card, access pass and lanyard is returned as soon as practicable.
- The individual's LEAP 'interest flag' or LEDR MK2 'Field Contact' must be immediately updated to 'inactive' by CSU.

10. End of service or termination process

- The relevant Victoria Police Contract Manager is responsible for ensuring that up to date records of service providers and external government agency and non-government personnel are maintained.
- Access to systems will be removed automatically in line with the end date in the engaging contract.
- The CSU must be advised in writing of a service provider's end of service in line with contractual obligations.
- Victoria Police issued Photo Identification, access pass and lanyard remain the property of Victoria Police and must be returned to the CSU at the end of service. The relevant Victoria Police Contract Manager is responsible for ensuring these items are returned.

Further advice and information

For further advice and assistance regarding this policy, contact SIPD, DSSD or using PBEA: [CONTRACTOR-SECURITY-MGR.](#)

Update history

DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
16/05/22	First issued.	FF-129775